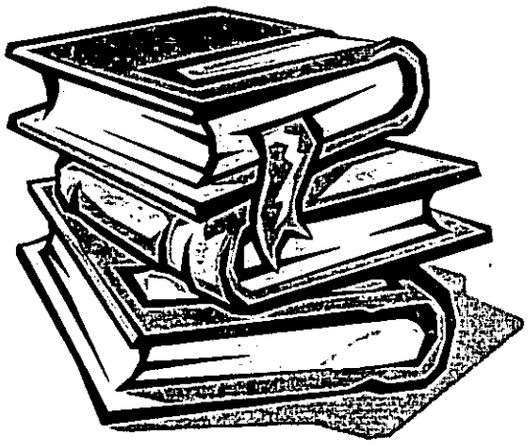
IT-3

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA E INFORMÁTICA

TRABALHO DE LICENCIATURA

SEGURANÇA DE COMPUTADORES



Supervisor:
Prof. DoutorYuri Petrossuiuk

Autor: *Guedes de Argentina Armando*
Maputo,Junho/2002

IT-3

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA E INFORMÁTICA

TRABALHO DE LICENCIATURA

SEGURANÇA DE COMPUTADORES

Supervisor:
Prof. DoutorYuri Petrossuiuk

Autor: *Guedes de Argentina Armando*

Maputo,Junho/2002

DEDICATÓRIAS/AGRADECIMENTOS

Quando lancei o desafio de fazer o Nível Superior tudo parecia um sonho irrealizável pois conjugar a minha vida de chefe de família, trabalhador e estudante, parecia ser uma amalgama confusa cuja separação não parecia fácil. Contudo com apoio e encorajamento das pessoas que me rodeiam decidi "tocar a bola para frente".

Chegado este dia olho para trás vejo todo caminho trilhado e digo valeu a pena.

Os meus sinceros agradecimento vão para:

***Ruth Matlava** minha Esposa, **Juliana, Hélio e Vera** meus filhos, pelo incansável encorajamento e alento que sempre me deram em todos os momentos, tornando assim este sonho realidade.

*Aos meus Pais **Armando Manuel, Vera Argentina**, aos meus **irmãos** e **restantes familiares** vai o meu especial reconhecimento.

* Ao **Sr. dr. Ângelo Azarias Chochava** (ex Secretário de Estado da Aeronáutica Civil) pelo grande esforço que empreendeu para a minha formação.

*Ao **Director Aníbal Samuel** e aos colegas da Escola Nacional de Aeronáutica, em especial a **Srª Adelaide Simeão**, pelo contributo incansável dispensado.

*Ao meu supervisor **Sr. Professor Doutor Yuri Petrossuiuk**, que sem o seu desmedido apoio e encorajamento este trabalho não seria possível.

*Aos meus **colegas de turma, professores** e **funcionários do DMI** e a título Póstumo ao colega **Samuel Este vão Manhanje** pelo grande apoio prestado durante o curso.

É sempre gratificante saber que sou capaz de colaborar com mais alguma coisa positiva para meu belo Moçambique que se pretende ver livre do analfabetismo e com uma massa intelectual sólida.

MUITO OBRIGADO

O estudante
Guedes de Argentina Armando

DECLARAÇÃO DE HONRA

Declaro por minha honra, que este trabalho é resultado da minha investigação que não foi submetido para outro grau que não seja o indicado "Licenciatura em Informática" na Universidade Eduardo Mondlane.

Maputo, Junho de 2002

O Estudante

Guedes de Argentina Armando

RESUMO

Os sistemas de informação representam, no presente, para a generalidade das empresas, uma verdadeira "espinha dorsal" de suporte a toda a actividade. A eficácia e fiabilidade dos Sistemas de Informação representam hoje uma condição vital do sucesso das empresas modernas e competitivas.

Durante a última década, o uso das tecnologias da informação aumentou extraordinariamente, não só pelo crescimento do número total de utilizadores, mas também pela grande variedade e sofisticação das aplicações desenvolvidas.

Em consequência, as empresas estão a tornar-se cada vez mais vulneráveis, fazendo com que eventuais desastres exponham a empresa a riscos de perda do controlo da informação dos seus utilizadores.

Esta transformação é posta em cena com recurso a tecnologias de comunicação e de informação que permitem colocar, ao alcance do nosso conhecimento individual e colectivo, as diversas informações sobre os acontecimentos, no momento em que têm lugar, acompanhadas de análise e comentários interpretando o seu sentido.

Produz-se, assim, um efeito de aceleração no processo de aquisição e transmissão do conhecimento, que torna as pessoas mais exigentes, informadas e formadas.

Contudo, mais informação pressupõe uma vasta e complexa rede de suporte, criação de novas aplicações informações e um sem número de utilizadores, com diferentes níveis de acesso aos dados. Este fenómeno, característico da Era da Informação, implica riscos, que têm que ser prevenidos e colmatados. É sobre este assunto que procurarei reflectir no presente trabalho onde-se faz um levantamento das principais causas que tornam tais tecnologias perigosas para a sociedade quando os pressupostos em termos de segurança não são a prior devidamente

equacionados e analisados os possíveis riscos, falar da **Segurança dos Computadores** significa ter em conta todos estes factores.

Numa abordagem mais especifica, falar de Moçambique é falar dum país que como muitos outros ainda esta a desabrochar nas tecnologias de tratamento e transmissão da informação computarizada, por isso vulnerável a violação da informação transmitida, dados os problemas que já são sabidos, tais como fraco domínio dessas tecnologias, fracos recursos financeiros entre outros.

O presente trabalho pretende despertar e fazer uma abordagem dessas questões todas chamando a atenção sobre os principais riscos e a maneira de os privar ou evitar.

Estou certo que abordei apenas uma parte do problema, numa vertente de um estudante, mas estou em crer que outros colegas o farão no futuro. Em termos escrutarias do trabalho, foquei na generalidade os seguintes aspectos: segurança básicas dos computadores e dos principais riscos, métodos criptográficos como ferramenta de segurança na transmissão de informação, as arquitecturas de seguranças e, finalmente, o uso da codificação como outro meio de segurança, mais concretamente os códigos com base irracional.

ÍNDICE

CONTEÚDO ..... PÁGINA

1.0 - OBJECTIVOS

1.1 - OBJECTIVOS GERAIS

Numa altura em que o computador entrou definitivamente na vida quotidiana dos moçambicanos, a generalização de programas e aplicações informáticas é uma realidade. Todos nós usamos computadores, directa ou indirectamente, em casa, no trabalho, ou em actividades da vida diária como a utilização de uma caixa multibanco que no passado não existia.
A informática está ao dispor de todos nós , e temos que tirar o máximo partido de tudo o que nos oferece.

A Internet, é o culminar de um processo de globalização da informação, numa época em que o computador é o meio de comunicação por excelência. Esta globalização iniciou-se com a rádio e as emissões em directo, a que se juntou a imagem da televisão , atingindo o seu auge ao permitir que todos possamos receber informação, em qualquer lugar , no país e do mundo, directamente da fonte, ou enviá-la, sem intermediários, sem censura.

Mas por ser um sistema deste tipo, interactivo, existem muitos perigos na sua utilização, até agora pouco divulgados em Moçambique, podendo causar danos, não só materiais, mas também éticos e morais, pelo que os utilizadores têm de ter o bom senso de não caírem na teia.
Começando pelos mais gerais, temos os custos de uma utilização compulsiva. É muito fácil passar horas a navegar na rede. Mas a navegação não é grátis.

Existem os riscos associados à transmissão e partilha de dados pessoais, estando associado um risco de violação de privacidade.

Por exemplo: temos os riscos associados à informação que pomos disponível na rede. Um exemplo típico, é a inserção dos dados dos cartões de crédito em operações de compra ou reserva de produtos, tais como, férias, hotéis e aluguer de viaturas. As compras na rede por aí fora, é preciso ter muito cuidado porque há muitas empresas fictícias.

Além destes, temos riscos associados à sociedade. Na Internet, há muitas páginas que colidem com as regras, o bom senso, e a educação das pessoas. Sendo necessário ter uma atenção especial à utilização da Internet pelas crianças, também ao nível informático existem aplicações para impedir o acesso a este tipo de páginas. Mas em ambos os casos, a informação é pouca, e como tal, a maior parte das pessoas estão sujeitas a estes riscos.

Os sistemas de informação representam, no presente, para a generalidade das empresas, uma verdadeira "espinha dorsal" de suporte a toda actividade. A eficácia e fiabilidade dos Sistemas de Informação representam hoje uma condição vital do sucesso das empresas, organizações.

Durante a última década, o uso das tecnologias da informação aumentou extraordinariamente, não só pelo crescimento do número total de utilizadores, mas também pela grande variedade e sofisticação das aplicações desenvolvidas.

Em consequência, as empresas estão a tornar-se cada vez mais vulneráveis, fazendo com que eventuais desastres exponham a empresa a riscos de perda do controlo da informação dos seus utilizadores.

Para minorar estes efeitos urge definir sistemas de segurança de fácil domínio e aplicabilidade.

O presente trabalho apresenta alguns deles que pela sua natureza já provaram serem sistemas altamente eficazes, e recomendáveis.

1.2 - OBJECTIVOS ESPECÍFICOS

Os objectivos específicos do presente trabalho prendem-se com os seguintes aspectos :

a) como usar o computador com segurança.

Este prevê algumas precauções básicas como seja o conhecimento claro dos riscos pontenciais de infecção dos computadores e a vulnerabilidade da rede em uso numa organização.

b) como prever a violação da segurança da rede informática instalada na organização.

Independentemente do tipo de controle exercido num sistema informático existe sempre uma manifesta tendência de violação da segurança da mesma por parte da outrem (interna ou externa). Pelo que é sempre importante que tais riscos sejam previamente tidos em conta com vista a minorar os riscos de uma possível violação.

c) avaliação permanente dos padrões de segurança dos computadores.

Como é sabido a informática é uma das ciências que nos últimos anos tem sofrido mutações progressivas. Dada a investigação científica permanente a que esta área está sujeita. Esta vertente implica uma actualização permanente dos níveis de segurança dos sistemas informáticos em função de tais alterações, dado que esta evolução é seguida também com evolução do métodos da violação da segurança dos computadores na esteira do crime informático que tende a subir galopatemente na arena internacional.

A título de exemplo após os ataques terroristas de 11 de Setembro de 2001 nos EUA, começaram a ser desenhados novos modelos de segurança em aeroportos de diversos países e em alguns centros informáticos estratégicos.

SEGURANÇA DE DADOS EM COMPUTAÇÃO

INTRODUÇÃO

A comunicação é a arte do transporte de informação de um ponto ao outro. A nossa vida quotidiana está cheia de formas de comunicação: A conversação, a imprensa, o telefone, a rádio, a televisão, etc.

Uma das características da sociedade humana é justamente a importância que dedica a esta arte e sem dúvida, a ela se deve a grande parte do progresso da humanidade.

Para levar a cabo este objectivo, é necessário produzir um fenómeno físico capaz de assumir configurações diferentes, as quais se associa o conteúdo dessa informação.

A informação desempenha um papel de capital importância na humanidade que com o avanço da tecnologia em especial na área de processamento de informação computorizada, se torna cada vez relevante o estudo e sistematização das técnicas mais eficientes para se alcançarem melhores sucessos.

Os técnicos preocupam se fundamentalmente em garantir que a transmissão do sinal de um ponto a outro se faça sem que o mesmo sofra sensível alteração, isto é o sinal informação de chegada seja replica perfeita do sinal (informação) de origem.

Contudo na transmissão analógica de informação a preocupação com a característica do sinal da informação não existe, ao passo que as técnicas digitais que envolvem frequentemente processamento dos sinais transmitidos de uma forma ou outra, interessando porém preservar o conteúdo da informação.

É em relação ao processamento digital, que actualmente usa o sistema de numeração binária para representação e processamento de informação e sendo importante realçar que o seu uso prende-se as circunstâncias históricas da época da criação dos computadores da segunda

geração, dado que do ponto de vista tecnológico teria sido muito difícil na época, a criação de dispositivos digitais que tivessem mais do que dois estados estáveis, tendo sido achado como sistema conveniente o sistema binário, actualmente o mais usado.

Um dos maiores problemas e um dos mais difíceis de resolver é o da segurança de dados. O problema tem muitas facetas e envolve as instalações físicas, procedimentos operacionais, características do hardware do computador e convenções do software e da programação.

Vivemos numa sociedade que se baseia em informações e que exibe uma crescente propensão para colectar e armazenar informações, daí a necessidade de se ter mecanismos de segurança realmente eficientes.

CAPÍTULO I

1. SEGURANÇA DE DADOS

A segurança de dados pode ser definida como a protecção de dados contra o acesso acidental ou intencional de pessoas não autorizadas, e contra alterações não permitidas, pelo principal usuário.

A segurança no universo computacional divide-se em **segurança lógica** e **segurança física**, presentes tanto em computadores e $P.C_S$ individuais assim como em computadores ligados em rede na Internet ou Rede interna (12).

1.1 - SEGURANÇA FÍSICA

Entende-se por **segurança física** aquelas ameaças sempre presentes, mas que nem sempre nos lembramos tais como: incêndios, desabamentos, relâmpagos, cheias, problemas na rede eléctrica, acesso indevido de pessoas ao Centro de Processamento de Dados, treina mento, ineficiente do pessoal, e outros (12).

Esta segurança pode ser feita através de medidas, tais como serviços de guarda, uso de no-breaks, alarmes e fechaduras, circuito interno de televisão e sistemas de escuta são realmente uma parte da segurança de dados. As medidas de protecção física são frequentemente citadas como "segurança computacional", visto que têm um importante papel também na prevenção do item acima exposto.

As técnicas de protecção de dados por mais sofisticadas que sejam, não tem serventia nenhuma se a segurança física não for garantida.

1.2 - SEGURANÇA LÓGICA

Outro aspecto não menos relevante é **a segurança lógica**, esta requer um estudo maior, pois envolve investimento em softwares de segurança ou elaboração dos mesmos.

Deve-se estar atento aos problemas causados por vírus, acesso de invasores de rede, programas de backup desactualizados ou feitos de maneira inadequada, distribuição de senhas de acesso, etc. (12)

Um recurso muito utilizado para se proteger dos invasores da Internet é a utilização de um programa de **criptografia** que baralha o conteúdo da mensagem, de modo que ela se torna incompreensível para aqueles que não sejam nem o receptor ou emissor da mesma. O presente trabalho mais adiante aborda outras formas de protecção, em uso e em desenvolvimento.

1. 3 - OBJECTIVOS

O objectivo da segurança de dados vai desde uma fechadura ou uma grade na porta da sala de computadores até o uso de técnicas criptográficas sofisticadas e códigos de autorização, muito bem elaboradas.

Seu estudo não abrange somente o crime computacional (hackers), envolve qualquer tipo de violação da segurança, como erros no processamento ou códigos de programação, mal definidos.

A segurança de dados tem por objectivo restringir o uso de informações (Software e dados armazenados) no computador e dispositivos de armazenamento associados por indivíduos seleccionados, preservação do património da empresa (os dados e as informações fazem parte do património).

Deve-se preservá-lo protegendo-o contra revelações acidentais, erros operacionais (montagem errada de um disco magnético, por exemplo) e contra as infiltrações que podem ser de dois tipos:

Infiltração deliberada: que tem como objectivos principais o acesso ás informações dos arquivos, descobrir os interesses da informação dos usuários, alterar ou destruir arquivos e obter livre uso dos recursos do sistema..

Infiltração activa: consiste desde o exame periódico dos conteúdos dos caixas de lixo da área do computador até à gravação clandestina dos dados armazenados que inclui:

1. acesso legítimo ao sistema para obtenção de informação não-autorizada;
2. Uso do disfarce: obtenção de identificação própria através de meios impróprios (como a gravação clandestina e compra da senha em circuitos ilícitos) seguindo-se depois o acesso ao sistema como um legítimo usuário.
3. Infiltrar-se através de canais activos de comunicações (ex: rede das T.D.M.)
4. Meios físicos: incluem o acesso ao sistema através de uma posição no centro de computação, ou seja, profissionais que ocupam cargos com acesso ao CPD e fornecem as informações a terceiros; e o roubo de meios removíveis de armazenamento.

1.3.1 - CAMINHOS PARA ALCANÇAR OS OBJECTIVOS DA SEGURANÇA:

1. Detecção e análise dos pontos vulneráveis do sistema computacional
2. Estabelecimento de políticas de segurança técnicas de segurança que incluam aspectos do hardware computacional, rotinas programadas e procedimentos manuais, bem como os meios físicos usuais de segurança local e segurança do pessoal, fechaduras, grandes, chaves e crachás.

- Execução das políticas de segurança
- Acompanhamento
- Avaliação dos resultados em relação aos objectivos traçados
- Correcção de objectivos e políticas
- Gerenciamento do acesso (12)

Trata-se da prevenção para que usuários não autorizados obtenham serviços do sistema computacional ou obtenham acesso aos arquivos. Este controle é um pouco mais complexo quando se trata de uma rede, já que qualquer um pode se fazer passar por usuário autorizado, bastando que obtenha as facilidades acima mencionadas, daí a importância do uso de técnicas de segurança, como senhas ou identificação por cartões magnéticos e outros.

1.4 - FACTORES A CONSIDERAR NO PLANO DE SEGURANÇA:

1) Conteúdo das informações

Refere-se à sensibilidade dos programas e dados que possam exigir um dos seguintes itens: nenhuma providência sobre segurança de dados, restrições normais a necessidades de conhecimento, ou preocupações extensas para evitar revelação.

2) Ambiente:

Refere-se aos usuários e aos métodos pelos quais eles têm acesso ao sistema.

3) Comunicações:

Referem-se ao uso das facilidades das comunicações de dados, que podem ser no local do computador, podem ser uma rede privada ou pode ser uma rede pública (ex: a rede das TDM).

4) Facilidades de sistema:

Referem-se a serviços previstos pelo sistema computacional que podem incluir, no mínimo, funções especializadas, solução de problema interactivo, apoio remoto de programação e um sistema total de informação.

No fundo, deve ser criado um Plano de Segurança (**como evitar problemas**).

O Plano de Contingência (**o que fazer em caso de problemas**).

É oportuno frisar que a segurança absoluta não existe - ninguém é imune a ataques nucleares, colisões com cometas ou asteróides, epidemias mortais (ex: sida), sequestros, guerras, cheias e outros

Trata-se de descobrir os pontos vulneráveis, avaliar os riscos, tomar as providências adequadas e investir o necessário para ter uma segurança homogénea e suficiente.

Perante o exposto várias perguntas podem ser colocada tais como.

Proteger

- O quê?
- De quem?
- A que custos?
- Com que riscos?

No mundo globalizado em que vivemos a resposta é só uma proteger é procurar preservar todos os elementos envolvidos no tratamento e transmissão da informação.

CAPÍTULO II

2 - PRINCÍPIOS BÁSICOS DE SEGURANÇA

Os princípios básicos de segurança a ter em conta nos sistemas são:

- **Confidencialidade**: protecção da informação compartilhada contra acessos não autorizados; obtém-se a confidencialidade pelo controle de acesso (senhas) e controle das operações individuais de cada usuário;
- **Autenticidade**: garantia da identidade dos usuários;
- **Integridade**: garantia da veracidade da informação, que não pode ser corrompida (alterações acidentais ou não autorizadas);
- **Disponibilidade:** prevenção de interrupções na operação de todo o sistema (hardware + software); uma quebra do sistema não deve impedir o acesso aos dados.

2.1 - SITUAÇÕES DE INSEGURANÇA E SUAS CAUSAS

As ameaças podem ser oriundas das seguintes situações de insegurança:

2.1.1 - CATÁSTROFES

- **Incêndio** acidental ou intencional;
- **Alagamento** por inundação das salas com risco potencial, por rotura dos tubos de água ou por cheias;
- **Explosão** intencional ou provocada por gás (em botijas);
- **Desabamento** parcial ou total do edifício onde se encontra o centro computacional.;
- **Grande sobrecarga** na rede eléctrica ou relâmpagos causando danos totais ou parciais nos equipamentos;
- **Guerras** - movidas por motivações políticas ou outros com consequências imprevisíveis.

2.1.2 - PROBLEMAS AMBIENTAIS

- **Variações térmicas** - excesso de calor causa tratamentos e destrói médias; excesso de frio congela fisicamente dispositivos mecânicos, como discos rígidos.
- **Humidade** – altera as características do funcionamento dos equipamentos.
- **Poeira** depositada nas cabeças de leitura e gravação dos drivers, pode destruir fisicamente um disquete ou uma fita.
- **Radiações** - além de causarem danos às pessoas, podem provocar problemas diversos em computadores (proximidade do equipamento informático em zona de irradiação de raios)
- **Ruído** causa estreasse e falta de concentração no pessoal, em operação.
- **Fumos** - a fumo do cigarro deposita uma camada de componentes químicos (ex-necotina) nas cabeças de leitura e gravação dos derives, que pode inviabilizar a utilização de disquetes e fitas; fumo provocado por incêndios próximos ao local do Centro de Processamento de Dados é muito mais perigoso, pois produz o mesmo efeito que o fumo do tabaco.
- **Magnetismo** - grande inimigo das médias os efeitos magnéticos, podem desgravar disquetes, fitas e discos rígidos
- **Trepidação** - pode soltar as placas encaixadas nos "slots" e componentes em geral colocados em soquetes, além de destruir discos rígidos

2.1.3 - SUPRESSÃO DE SERVIÇOS

- **Falha de energia eléctrica** - grande risco potencial, à medida que paralisa totalmente todas as funções relacionadas à informática
- **Queda nas comunicações** - grande risco potencial, pois isola o cite do resto do mundo; risco de perda de dados
- **Ante nos equipamentos** - problema bastante comum, resolvido com backup de informações e de hardware
- **Ante na rede** - isola um ou mais computadores de um mesmo cite; risco potencial de perda de dados

- **Problemas nos sistemas operacionais** - risco potencialmente explosivo, pois podem comprometer a integridade de todos os dados do sistema e até mesmo inviabilizar a operação; elimina a confiança da equipe
- **Problemas nos sistemas corporativos** - grande risco, causam grande transtorno e perdas de dados
- **Paragem do sistema** - igualmente um grande risco

2.1.4 - COMPORTAMENTO ANTI-SOCIAL

- **Paralisações e greves** - problema contornável se houver uma condução política adequada
- **Invasões** - As invasões num sistema computorizado constituem um altíssimo risco de destruição acidental ou intencional.
- **Hacher** - é a pessoa interessada em testar e recondicionar qualquer tipo de sistema operacional. Muitos deles são programadores e possuem alto grau de conhecimento nos sistemas operacionais. Eles descobrem falhas nos sistemas e as razões pelas quais foram detectadas. Hacher constantemente procuram por conhecimento, compartilham gratuitamente o que descobrem e nunca têm a intenção de destruir arquivos ou sistemas.
- **Craker** - é um indivíduo que utiliza a sua sabedoria para comprometer a segurança da rede. Muitos deles possuem alto grau de conhecimento em linguagens de programação e de sistemas operacionais. Suas actividades incluem acesso não autorizado, danificar todo e qualquer tipo de sistema, espionagem etc. Geralmente tais actividades são tidas como ilegais e possuem sanções previstas em lei.

Phreaker

- Aquele que quebra a rede telefónica, por exemplo, para realizar ligações interurbanas gratuitas.

Sneacher

- Indivíduo contratado para penetrar no sistema visando testar a sua segurança

Empregado demitido ou descontente

- As estatísticas informam que grande parte dos acessos indevidos na empresas são feitos pelos próprios funcionários e os estragos foram grandes; é inevitável ter-se directivas para esta situação.

Espião

- A espionagem patrocinada pela concorrência nos negócios já atinge até interesses do estado. O grau de sofisticação da protecção vai depender do valor do bem a ser protegido. Os Bancos têm o problema mais complicado pois demandam ao mesmo tempo privacidade e disponibilidade dos mesmos dados. A única solução é investir mais forte na segurança.
- **Alcoolismo e drogas** - risco de comportamento anómalo de funcionários, com consequências imprevisíveis
- **Disputas exacerbadas** entre pessoas podem levar à sabotagem e alteração ou destruição de dados ou de cópias de segurança
- **Falta de espírito de equipe** - falta de coordenação, onde cada funcionário trabalha individualmente; risco de omissão ou duplicação de procedimentos
- **Inveja pessoal/profissional** - rixas entre funcionários, sectores, gerências, directorias mesmo caso do item anterior, porém de consequências mais intensas e pode levar a destruição dos dados.

2.1.5 - ACÇÃO CRIMINOSA

- **Furtos e roubos** - consequências imprevisíveis, podem inviabilizar completamente os negócios da empresa
- **Fraudes** - modificação de dados, com vantagens para o elemento agressor
- **Sabotagem** - modificação deliberada de qualquer activo da empresa
- **Terrorismo** - de consequências imprevisíveis, pode causar mortes, a destruição total dos negócios ou de mesmo de toda a empresa
- **Atentados** - uso de explosivos, com as mesmas consequências do item anterior
- **Sequestros** - acção contra pessoas que tenham alguma informação sobre Centro de Processamento Dados.
- **Espionagem industrial** - captação não autorizada de software, dados ou comunicação para uso de outrem.
- **Cracker** - indivíduo que conhece profundamente um computador e um sistema operacional e invade o cite com finalidade destrutiva.

2.1.6 - INCIDENTES VARIADOS

- **Erros de usuários** - de consequências imprevisíveis, desde problemas insignificantes até a perda total de informação; erros de usuários costumam contaminar as cópias de segurança (backup) quando não detectados a tempo
- **Erros em backups** - risco sério de perda de dados; o backup sempre deve ser verificado
- **Uso inadequado dos sistemas** - normalmente ocasionado por falta de Treinamento, falta de documentação adequada do sistema ou falta de capacidade de quem utiliza o sistema de forma inadequada; tem os mesmos riscos do item Erros de usuários
- **Manipulação errada de arquivos** - costuma causar perda de arquivos e pode contaminar as cópias de segurança
- **Treina mento insuficiente** - inevitavelmente causa erros pelo uso inadequado do software ou do equipamento.
- **Ausência/demissão de funcionário** - é problemático se a pessoa ausente for a única que conhece determinados procedimentos no CPD.
- **Estrasse/sobrecarga de trabalho** - uma pessoa sobrecarregada é mais propensa a cometer erros e adoptar atitudes anti-sociais por fadiga.
- **Equipe de limpeza** - deve receber o Treina mento adequado sobre segurança para evitar que este mexam os equipamentos de qualquer maneira (ex: desligar e ligar a ficha dos mesmos).

2.1.7 - CONTAMINAÇÃO ELECTRÓNICA

- **Vírus** - programa que insere uma cópia sua ou outros programas executáveis ou no sector de boom; os vírus se multiplicam através da execução do programa infectado
- **Bactéria** - programa de auto produção que vai consumindo recursos do processador e memória com o tempo.
- **Verme** - programa que se reproduz através de redes
- **Cavalo de Tróia** - programa aparentemente inofensivo e útil, mas que contém um código oculto indesejável ou danoso

- **Amiba** - usuário que, sem ter conhecimento para tanto, mexe na configuração do computador ou do software, causando problemas, perda de dados, tratamento da máquina, etc.
- **Falhas na segurança dos serviços** - os serviços da Internet são potencialmente sujeitos a falhas de segurança, basicamente devido ao fato de o UNIX ter sido gerado em ambiente universitário, que visava um processamento cooperativo e não a segurança; além disto, o UNIX é muito bem conhecido por hackers e crackers

CAPÍTULO III

3 - TIPOS DE ATAQUES

3.1 - FALHAS DE PROTOCOLOS

Gera uma família de ataques chamados DOS (negação de serviço), os hostes atacados reinicializam ou tem a sua performance prejudicada. O ataque LAND onde um invasor emite pacotes de requisição de conexão com endereços IPs de origem e destino iguais é um dos mais conhecidos.

3.2 - SPOOFING

Spoofing é o acto de usar uma máquina para personificar outra. Isso é feito forjando o endereço de origem de um ou mais Hosts empenhados na autenticação das máquinas individualmente. Para realizar uma sessão bem sucedida de spoofing, alguns crakers temporariamente `matam` ou anestesiam a máquina que eles estão personificando.

Se há interfaces de rede entre o atacante e o alvo, o atacante estará desperdiçando tempo (por exemplo, os pacotes têm de cruzar um hum inteligente, uma ponte ou um troteador, o spoofing provavelmente falhará).

3.3 - VAZAMENTO DE INFORMAÇÃO

O vazamento remoto de informações é obtido através da resposta a consulta de Pingo, Traceroute, Telnet, SNMP etc. A coleta de informações relativas a versões de sistemas operacionais e Hosts dão ao invasor informações que o permitirá planear os ataques a rede.

3.4 - INTERRUPÇÃO DE SERVIÇO

Os ataques de interrupção de serviço geralmente desactivam um ou mais serviços de rede. Este tipo de ataque, pode forçar a reinicializar ou reiniciar vários serviços. E, embora isso não seja um

risco importante de segurança, tempo de paralização (downtime) pode ser precioso. É um ataque praticamente sem defesa.

3.5 - BUGS E BACKDOORS

Os buas são defeitos em software ou protocolos e são explorados com a finalidade de ganhar roto em uma máquina (Deus) e aí pode fazer tudo; backdoors são abertas por default que as vezes (ou muitas) os administradores de sistema esquecem de desativá-las e assim temos um sistema aberto a quem quiser entrar.

3.6 - MAIL BOMB

É uma série de mensagens (milhares), enviadas a uma caixa postal. O objectivo do atacante é apenas enviar lixo para a caixa postal de alguém, congestionar a via de acesso corporativo à Internet. Existem diversos programas que automatizam o mail bombing.

Esquemas de exclusão e mail filtres são as únicas maneiras de evitar o mail bombing. Pode levar o Mail servir a um colapso gerando negação de serviço.

3.7 - CAVALOS DE TRÓIA

O termo vem de uma passagem da Ilíada de Homero, na qual os gregos deram de presente um imenso cavalo de madeira a seus inimigos, os troianos, aparentemente como oferta de uma proposta de paz.

Porém, após os troianos terem arrastado o cavalo para dentro das paredes da cidade, soldados gregos que estavam escondidos na barriga oca do cavalo, saíram à noite e abriram as portas da cidade permitindo a seus compatriotas invadir e capturar a cidade.

Por analogia, hoje na informática, o termo trojan ou cavalo de Tróia é usado para designar uma categoria de programas destruitivos mascarados em programas e aplicativos benignos.

3.8 - SCANNERS DE PORTAS

Os scanners são programas que buscam portas TCP abertas por onde pode ser feita uma invasão. Para que a varredura não seja percebida pela vítima, alguns scanners testam as portas de um computador durante muitos dias em horários aleatórios.

3.9 - SMURF

O surf é outro tipo de ataque de negação de serviço. O agressor envia solicitações Pingo (um teste para verificar se um serviço da Internet esta acessível) para um endereço de broadcast. Usando spoofing, o cracker faz com que o servidor de broadcast encaminhe as respostas não para seu endereço, mas para o da vítima. Assim o computador-alvo é inundado pelo Pingo.

3.10 - SNIFFING

O sniffer é um programa ou dispositivo que analisa tráfego de rede. Sniffers são úteis para gerenciamento de redes, mas nas mãos crackers permitem roubar senhas e outras informações sigilosas.

3.11 - MAN IN THE MIDDLE

Ataque que envolve a conversação completa entre o atacante e o atacado, tem controle sobre uma máquina no caminho entre atacado e atacante, altera a rota entre atacado e atacante. Defesa: Evite ao máximo a libertação de serviços perigosos em máquinas externas através de brechas em filtros.

3.12 - PING OF DEATH

Ele consiste em se enviar um pacote IP com tamanho maior que o máximo permitido (65535 bytes), para a máquina que se deseja atacar. O pacote é enviado na forma de fragmentos (a razão é que nenhum tipo de rede permite o tráfego de pacotes deste tamanho) e quando a

máquina destino tenta montar fragmentos, inúmeras situações podem ocorrer; a maioria das máquinas trava, algumas reinicializam, outras abortam e mostram mensagens na consola, etc.

Praticamente todas as plataformas eram afectadas por este ataque, e todas as que não tiveram correcções de segurança instalados, ainda o são. Este ataque recebeu o nome de Pingo O`Death porque as primeiras ocorrências deste ataque foram a partir do programa pingo, entretanto, qualquer pacote IP com mais de 65535 (pacote inválido) provoca o mesmo efeito.

3.13 - ATAQUE DE REPLAY

Forma particular de ataque em que parte de uma transmissão de rede é gravada e reproduzida posteriormente. Normalmente, esse tipo de ataque está associado a uma criptografia mal-estruturada. Exemplo: um mecanismo de autenticação transmite pela rede uma credencial para um usuário.

Se a credencial for codificada sempre da mesma maneira, o atacante poderá gravar a sequência criptografada e incorporá-la numa transmissão realizada por ele mesmo. Sem saber a senha, ele seria capaz de conseguir acesso ao sistema.

Um esquema de criptografia projectado correctamente deverá modificar a forma de codificação de qualquer credencial, não permitindo que haja duas instâncias iguais e garantindo que a repetição de uma forma anterior não tenha sucesso.

3.14 - DENIAL OF SERVICE (DOS)

Ataque que consiste em sobrecarregar um servidor com uma quantidade excessiva de solicitações de serviços. Há muitas variantes como os ataques distribuídos de negação de serviço (DOS) que paralisam vários cites ao mesmo tempo. Nessa variante, o agressor invade muitos computadores e instala neles um software zumbi, como o Tribal Flood ou o trinco. Quando recebem a ordem para iniciar o ataque, os zumbis bombardeiam o servidor alvo, tirando-o do ar.

CAPÍTULO V

4 - PREJUÍZOS DE CORRENTES DA FALTA DE SEGURANÇA

A Informática é o centro chave da empresa ou organização. Qualquer pequeno problema no(s) servidor(es) corporativo(s) ou em algum servidor departamental pode paralisar vários ou mesmo todos os departamentos da empresa. Quanto maior o grau de integração dos sistemas, quanto maior o volume e a complexidade dos procedimentos ou negócios, maior será a dependência em relação à Informática.

Podemos classificar os prejuízos decorrentes de problemas, conforme a abrangência dos danos e as providências tomadas para retornar à normalidade assim temos os seguintes tipos de prejuízos:

4.1 - QUANTO AOS GRAUS DE SEVERIDADE

4.1.1 - INSIGNIFICANTES

Os casos em que o problema ocorre, é detectado e corrigido sem maiores repercussões. São problemas isolados, sem nenhuma repercussão na estrutura computacional da empresa, ou organização. O maior prejuízo é a despesa com a mão de obra alocada, ou algum sofrimento desperdiçado exemplo presença de um vírus num computador, que é prontamente detectado e exterminado. Certamente é necessário um grande investimento em segurança para que os problemas possam ser prontamente resolvidos e os prejuízos minimizados;

4.1.2 - PEQUENOS

O problema ocorre, existe uma pequena repercussão na estrutura computacional e organizacional da empresa (atrasos, bloqueio de sistema, perdas de movimentação, etc.), e o problema é resolvido. Um exemplo é a perda dos dados corporativos, a recuperação via backup da posição anterior e a necessidade de redigitação da movimentação de um dia. (bancos e outros serviços),

ou, então, a destruição física, acidental ou propositada, de um servidor corporativo, com a necessidade de substituição de emergência, mas sem perda dos dados. Os prejuízos são restritos ao âmbito da empresa, sem repercussões nos seus negócios e sem interferências com seus clientes;

4.1.3 - MÉDIOS

O problema ocorre, provoca repercussão nos negócios da empresa e interfere com os seus clientes, mas a situação consegue ser resolvida de maneira satisfatória, normalmente com um grande esforço e com maior ou menor desgaste interno e externo da empresa. Exemplos: erros graves na facturação, perda de dados sem backup entre outros.

4.1.4 - GRANDES

Repercussões irreversíveis de carácter interno ou externo, com perda total de dados, prejuízo financeiro irrecuperável, perda de clientes, perda da imagem, paragem da Empresa ou organização e perda da posição no mercado podendo na maioria dos casos conduzir a empresa a falência, e com contenciosos em juízo movidos pelos clientes lesados.

Alguns métodos de protecção de informação mais usados são:

- **A CRIPTOGRAFIA E OS FIREWALLS**

Começaremos por apresentar uma abordagem sobre a criptografia sem contudo descorar a grande importância que os Firewalls desempenham na segurança de dados nas redes de computadores.

CAPÍTULO V

5 - CRIPTOGRAFIA

Os profissionais de Informática se deparam com o desafio, sempre crescente, de avaliar, implantar e manter confiabilidade nos serviços oferecidos pelos sistemas integrados por telecomunicações e redes de computadores com que trabalham. Com o avanço das tecnologias da informação há um aumento na sua gama de aplicações, mas também nas formas e possibilidades de uso impróprio, desvios, sabotagens, fraudes, vandalismos, colapsos, bloqueios indevidos, efeitos que compromentem a confiança de clientes e da sociedade no uso dessas tecnologias, como também suas expectativas quanto ao papel do computador no futuro da nossa civilização.

A história da Criptografia moderna revela quão fascinante tem sido a aventura desse desafio, e quão proficuo é o legado das ciências matemáticas aplicadas na protecção à informação, veiculada e um meio tão diáfano, por onde é electronicamente é transmitida. A criptografia nos fornece os elementos - os algoritmos e protocolos - para construção de mecanismos de protecção a aplicações sensíveis, como por exemplo o comércio electrónico ou as redes privadas virtuais (VPNs). Entretanto, a criptografia aborda apenas a parte fácil desse desfio.

O uso seguro de sistemas de informação que funcionam por meio de canais inseguros, demanda não só esforços gerenciais e motivacionais, além de medidas de protecção, de salvaguarda, de controle e de auditoria, mas demanda antes e principalmente, um quadro claro com as fronteiras entre ameaças defensáveis, detectáveis, viáveis e imagináveis ao sistema que se quer proteger. Para termos êxito ao traçar tal quadro, é necessário distinguirmos os conceitos de **Segurança** e **Protecção**.

Segurança assemelha-se ao conceito de quantidade, que deve permear toda a concepção e evolução de um projecto. **Protecção** assemelha-se a trancas, grades ou fechaduras, mecanismos instalados no final da implementação de um projecto arquitetônico que tenha previsto

integralmete a função, utilidade e manutenção de cada um destes mecanismos. Segurança é processo, protecção é acção mensurável. Protecção se instala, segurança planeia-se. **Protecção é defesa, segurança é processo**. Segurança na informática está relacionada à confiança que se pode ter nos canais electrônicos de comunicação de dados, operando num contexto onde outros canais, no mundo da vida, deles se valem para transmitir significados.

A criptografia é a área da matemática e da engenharia que oferece técnicas de protecção a mecanismos de acesso e à integridade de dados, e ferramentas de avaliação da eficácia dessas técnicas. Estas técnicas e ferramentas são de natureza puramente sintática, não podendo portanto serem destinadas a fornecer ou induzir, por si mesmas, confiança no significado da informação que tais dados supostamente veiculam. A criptografia pode oferecer segurança à informática, mas somente onde e quando a confiança no significado da informação veiculada pelos dados que protege já tenha sido obtida ou fornecida por outros meios.

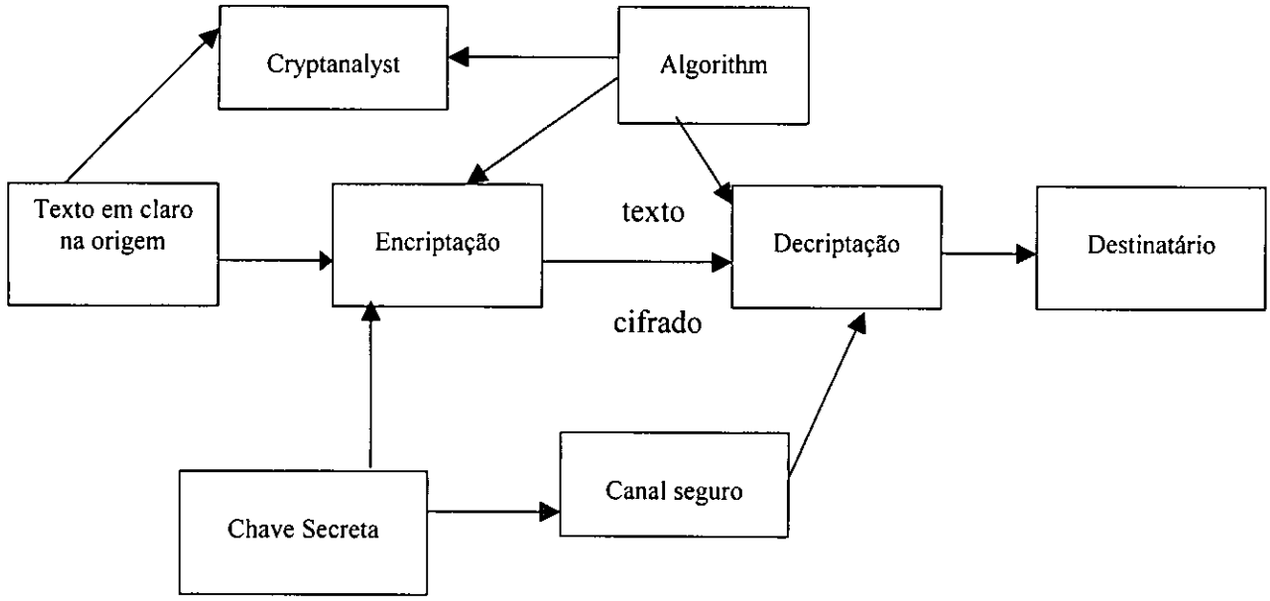
5.1 - SISTEMAS CRIPTOGRÁFICOS

Pensando na necessidade de se criarem ferramentas capazes de proteger a informação e de prover segurança aos dados armazenados e transmitidos pelas organizações através do mundo, veio a motivação para se estudar Criptografia crê-se que através desta disciplina podem-se criar aplicações que dêem maior segurança às informações digitais.

Criptografia, do grego Kryptos (escondido, oculto) mais a palavra grafia (grafa, escrita), é a ciência de escrever em códigos ou em cifras, ou seja, através de uma série de procedimentos transforma-se um texto "em claro"(inteligível) num texto "cifrado"(ininteligível). Outro conceito relacionado a criptografia é o da Criptoanálise, do grego krypto, mais a palavra análysis (decomposição), é a ciência (embora muitos estudiosos digam que está é mais para a arte do que para a ciência) que estuda a decomposição do que está oculto ou a "quebra"do sistema criptográfico. **Finalmente define-se Criptologia como a ciência que engloba a criptografia e a criptoanálise.**

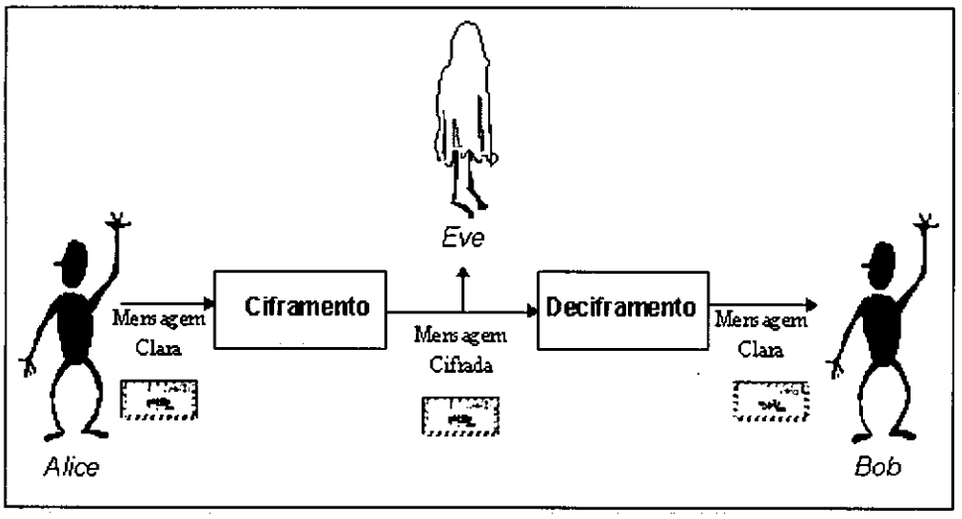
Existem dois tipos básicos de Sistemas Criptográficos, o chamado simétrico ou de chave única e o chamado Assimétrico ou de chave pública, ambos serão abordados, neste trabalho.

5.1.2 - CRIPTOGRAFIA USANDO SISTEMA SIMÉTRICO OU DE CHAVE ÚNICA.



A história da criptografia e chave única confunde-se com a própria história da criptografia. Desde a chamada era da criptografia pré-computacional que sistemas criptográficos são baseados em chaves ou senhas. Porém, naquela época, essas chaves eram grupos de até 6 caracteres (normalmente letras de algum alfabeto) que eram utilizados para a cifragem de alguma mensagem. Desde quando se tem notícia, a criptografia (também conhecida como criptografia baseada na obscuridade), trabalhava baseada no falso princípio de que um sistema estaria seguro na medida em que ninguém, excepto seus criadores, tivessem acesso a informação sobre seu mecanismo interno. Como exemplo, pode-se mostrar o cifra dor de César, o imperador romano que se utilizava dele para mandar mensagens a seus generais. Este Cifrador funciona substituindo um carácter da mensagem por outro que estivesse três posições a frente do substituído. Com método assim, qualquer um que analisasse os textos ou mensagens cifradas, poderia, com um pouco de tempo, descobrir o texto original e quebrar o método utilizado bastando para isso usar o algoritmo adequado.

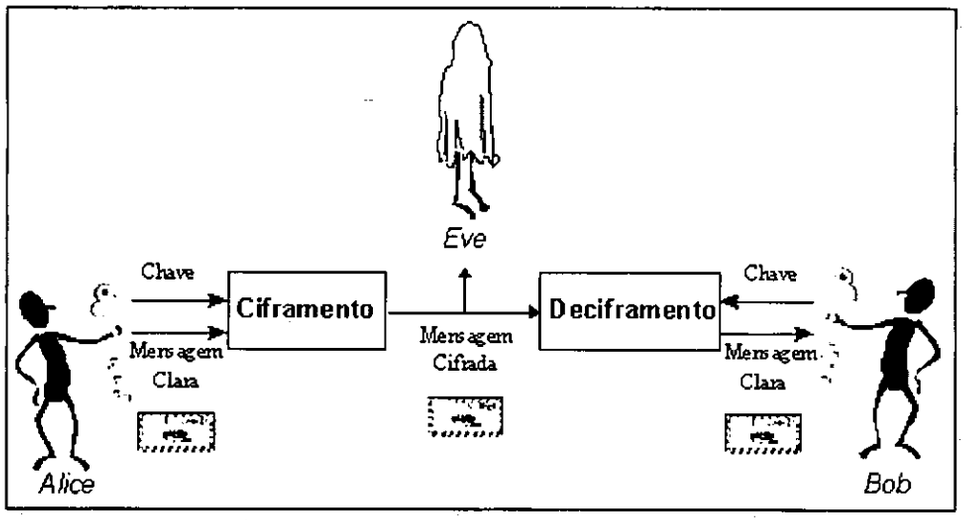
Com o advento dos computadores, a criptografia modificou a maneira de ser executada. Com a moderna, um sistema não deve poder ser quebrado nem mesmo pelo seu criador, e isso se consegue através da utilização de chaves. Para cifrar uma mensagem utiliza-se uma ou mais chaves (sequência de caracteres) que serão embaralhadas com o texto ou mensagem original. Estas chaves devem ser mantidas em segredo, pois somente com o conhecimento delas é que se poderá decifrar a mensagem. Assim sendo, o primeiro tipo de algoritmo que surgiu foi o de chave única. Entende-se por chave secreta ou chave única aquela que o ciframento de uma mensagem baseia-se em dois componentes: um *algoritmo* e uma *chave*. Um *algoritmo* é uma transformação matemática. Ele converte uma mensagem em claro em uma mensagem cifrada e vice-versa. Quando *Alice* (origem)cifra uma mensagem, ela utiliza um algoritmo de ciframento para transformar o conteúdo em claro da mensagem em texto cifrado. Quando *Bob* (destinatário) decifra uma mensagem, ele utiliza o algoritmo de deciframento correspondente para converter o texto cifrado de novo em uma mensagem clara.



Antigamente, a segurança do ciframento estava baseada somente no sigilo do algoritmo criptográfico. Se *Eve* (um intruso) conhecesse o algoritmo sem chave, poderia decifrar uma mensagem cifrada tão facilmente quanto *Bob*. Pode-se contornar o problema apresentado utilizando o segundo componente básico da criptografia de mensagens: a chave. Uma chave é uma cadeia aleatória de bits utilizada em conjunto com um algoritmo. Cada chave distinta faz com que o algoritmo trabalhe de forma ligeiramente diferente.

Embora existam algoritmos que dispensem o uso de chaves, sua utilização oferece duas importantes vantagens. A primeira é permitir a utilização do mesmo algoritmo criptográfico para a comunicação com diferentes receptores, apenas trocando a chave. A segunda vantagem é permitir trocar facilmente a chave no caso de uma violação, mantendo o mesmo algoritmo.

O número de chaves possíveis depende do tamanho (número de bits) da chave. Por exemplo, uma chave de 8 bits permite uma combinação de no máximo 256 chaves (2^8). Quanto maior o tamanho da chave é mais difícil quebrá-la, pois estamos aumentando o número de combinações.



Quando *Alice* cifra uma mensagem, ela utiliza um algoritmo de ciframento e uma chave secreta para transformar uma mensagem clara em um texto cifrado. *Bob*, por sua vez, ao decifrar uma mensagem, utiliza o algoritmo de deciframento correspondente e a mesma chave para transformar o texto cifrado em uma mensagem em claro. *Eve*, por não possuir a chave secreta, mesmo conhecendo o algoritmo, não conseguirá decifrar a mensagem. A segurança do sistema passa a residir não mais no algoritmo e sim na chave empregada. É ela que agora, no lugar do algoritmo, deverá ser mantida em segredo por *Alice* e *Bob*.

Quando a chave de ciframento é a mesma utilizada para deciframento ou esta última pode facilmente ser obtida a partir do conhecimento da primeira, ambas precisam ser compartilhadas previamente entre origem e destinatário, antes de se estabelecer o canal criptográfico desejado,

utilizando-se um canal seguro e independente do destinado à comunicação sigilosa. Este tipo de ciframento emprega a criptografia conhecida como *simétrica* ou de chave secreta.

Um sistema com algoritmo de chave única tem como vantagem ser muito mais rápido na cifragem e decifragem do que os sistemas que utilizam chave pública, e também poder ser implementado em hardware, por ser extremamente flexível.

Os sistemas que utilizam chave única são os mais adequados para criptografia off-line, onde o usuário necessita apenas armazenar localmente seus arquivos cifrados e transmití-los, se for o caso, através de outros meios.

A maior, talvez única, desvantagem desses tipos de sistemas é a distribuição de chaves a qual deve ser feita por meio de um canal seguro ou com a utilização, pelo sistema, de protocolos de distribuição muito complexos de serem implementados.

5.2 - ALGORITIMO CRIPTOGRAFICO SIMÉTRICO OU DE CHAVE SECRETA

Um dos algoritmos criptográficos modernos que nos vamos referir o DES (Data Encryption Standard) derivado de uma proposta da IBM, chamado lucifer e adoptado para NBS (Nacional Bureau ou Standards) em 1976 para uso em comunicações governamentais não classificadas.

No início a sua introdução foi acompanhada por bastante controvérsia com relação ao seu papel, mais concretamente em algumas grandes organizações da época como por exemplo a NSA, e NBS.

Na versão original de lucifer tinha uma chaves de 128 bits que por recomendações de NSA e NBS furão reduzidas para 52 bits sem nunca ter havido uma explicação plausível e clara sobre essa mudança.

Contudo hoje em dia o DES é o criptosistema mais usado no mundo apesar do esforço de algumas organizações como NSA para o retirar dada a sua avançada idade.

Descrição

O DES é um ciframento composto que cifra blocos de 64 bits (8 caracteres) em blocos de 64 bits, para isso ele se utiliza de uma chave composta por 56 bits mais 8 bits de paridade (no total são 64 bits também). Assim, para cada chave, o DES faz substituição monoalfabética sobre um alfabeto de 264 letras. A rigor, é uma substituição monoalfabética, mas as técnicas publicadas de quebra de substituições monoalfabéticas se aplicam apenas a alfabetos pequenos.

Basicamente o DES funciona através dos seguintes passos:

1. Uma substituição fixa, chamada de permutação inicial, de 64 bits em 64 bits;
2. Uma transformação, que depende de uma chave de 48 bits, e que preserva a metade direita;
3. Uma troca das duas metades de 32 bits cada uma;
4. Repetem-se os passos 2 e 3 durante 16 vezes;
5. Inversão da permutação inicial.

Os blocos que constroem o algoritmo são permutações, substituições de "ou exclusivo". As permutações do DES são de três tipos: na primeira, os bits são simplesmente reordenados (straight permutation); na segunda, alguns bits são duplicados e então reordenados (expandes permutation), aumentando assim o número de bits na saída; na terceira, alguns bits são descartados para depois reordenar os restantes (permute coice), diminuindo os bits de saída.

As substituições no Dês são conhecidos como S-boxes (Caixas S - caixas de substituição) e são especificadas em 8 tabelas onde entram blocos de 6 e saem blocos de 4 bits. O primeiro e o último bit são tomados como se fossem um número de 2 bits, formando assim as linhas das tabelas das caixas S. Os bits 2 a 5 agrupados formam um vector de 0 a 15.

Passa-se a ter, então, uma tabela onde a primeira linha é formada por números decimais que são representados por 4 bits (os quatro bits do meio dos 4 bits de entrada), e a primeira coluna é formada por números decimais que possam ser representados em 2 bits (os bits dos extremos do bloco de 6 bits de entrada). Para cada uma das caixas S, a combinação dos 4 bits do meio com os 2 bits das pontas fornecerá 4 bits conforme a tabela da caixa.

5.2.1 - SEGURANÇA DO DES

No caso do DES, várias tentativas de quebra (criptoanálise) já foram publicadas. O DES pode ser quebrado pelo método da "força bruta", tentando-se todas as combinações possíveis para a chave. Como a chave é de 56 bits, tem-se um total de 256 chaves possíveis, ou aproximadamente 1017 possibilidades.

Porém, Diffie e Hellman conjecturam a construção de uma máquina especial de 1012 cifra mentos por segundo, que examinaria as possibilidades em um dia; a máquina conteria 106 chis, cada eliminando uma parte diferente do espaço de chaves. A máquina custaria em torno de 20 milhões de dólares, com um custo diminuído para algumas centenas de milhares de dólares até o final da década de 80.

A questão da segurança do DES criou polémica desde sua criação. Existem muitas especulações, inclusive sobre a existência de uma trapo dor ("porta dos fundos" uma entrada por onde seria fácil o deciframento por parte do governo americano através da NSA) e também a respeito do número de bits da chave, do número de interacções, do formato das caixas S e uma série de problemas que foram apontados já na época da publicação do algoritmo e até bem pouco tempo atrás ainda não passavam de especulações.

5.2.2 - CHAVES FRACAS

Por causa da modificação inicial que a chave sofre, transformando-se em duas subchaves que são usadas em partes diferentes do algoritmo, o DES corre o risco de trabalhar com as chamadas chaves fracas.

Inicialmente o valor da chave é dividido em duas metades as quais vão sofrer deslocamentos separadamente. Se todos os bits de cada metade forem 0 ou 1, então a chave usada para qualquer ciclo do algoritmo será a mesma usada para qualquer outro ciclo do algoritmo. Isto pode ocorrer se a chave for inteiramente formada por 1 ou inteiramente por 0 ou metade por 1 e metade por 0.

Com isso, existem pares de chaves [A, B] onde A cifra um texto em claro e tanto A quanto B são capazes de decifrar o criptograma cifrado por A.

5.2.3 - TAMANHO DAS CHAVES

Quando a IBM criou o LUCIFER, ele tinha uma chave de 128 bits. Alguns anos depois, quando da criação e padronização do DES a chave utilizada para algoritmos criptográficos caiu para 58 bits. Muitos criptólogos da época argumentaram que deveria ser aumentado o número de bits da chave para dificultar a utilização do método da força bruta.

Em 1981, Diffie e Hellman disseram que, com a evolução da tecnologia computacional, principalmente no que diz respeito a capacidade de armazenamento e de processamento, no ano de 1990 o DES seria um algoritmo completamente inseguro. E realmente, em 1990, uma dupla de Israelitas, Bicham e Shamir, descobriram e publicaram uma técnica nova: a criptoanálise diferencial (que será explicada posteriormente neste trabalho).

5.2.4 - NÚMEROS DE INTERAÇÕES

Através dos anos, existiram vários ataques bem sucedidos contra variantes do DES com interacções. Em 1982 o DES foi facilmente quebrado com 4 interacções, alguns anos depois o mesmo ocorreu para 6 interacções. A teoria de Shamir e Bicham explica que o DES com menos de 16 bits é mais facilmente quebrado pelo método do texto conhecido do que pela força bruta.

5.2.5 - ESTRUTURA DAS CAIXAS

Além da acusação de reduzir o tamanho da chave, a NSA foi também acusada da modificação da estrutura das caixa S. Vários criptólogos chegaram a conclusão que a NSA desenhou as caixas S para esconder uma "traz dor", deixando uma porta aberta apenas para eles entrarem. Vide Anexo I (Quadro Resumo do Algoritmo Simétrico).

Alguns Problema com DES

Apesar de sua simplicidade, existem alguns problemas na criptografia simétrica:

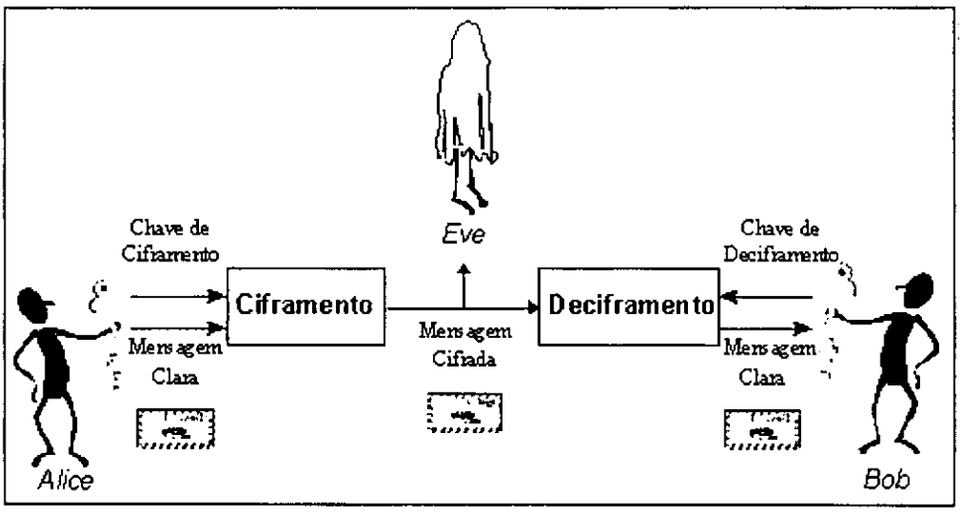
Como cada par necessita de uma chave para se comunicar de forma segura, para uma rede de n usuários precisaríamos de algo da ordem de n^2 chaves, quantidade esta que dificulta a gerência das chaves;

A chave deve ser trocada entre as partes e armazenada de forma segura, o que nem sempre é fácil de ser garantido;

A criptografia simétrica não garante a identidade de quem enviou ou recebeu a mensagem (autenticidade e não-repudiação).

5.3 - CRIPTOGRAFIA ASSIMÉTRICA OU DE CHAVE PÚBLICA:

A maneira de contornar os problemas da criptografia simétrica é a utilização da criptografia assimétrica ou de chave pública. A criptografia assimétrica está baseada no conceito de par de chaves: uma chave privada e uma chave pública. Qualquer uma das chaves é utilizada para cifrar uma mensagem e a outra para decifrá-la. As mensagens cifradas com uma das chaves do par só podem ser decifradas com a outra chave correspondente. A chave privada deve ser mantida secreta, enquanto a chave pública fica disponível livremente para qualquer interessado.



De uma forma simplificada, o sistema funciona assim: *Bob* e todos os que desejam comunicar-se de modo seguro geram uma chave de ciframento e sua correspondente chave de deciframento. Ele mantém secreta a chave de deciframento; esta é chamada de sua *chave privada*. Ele torna pública a chave de ciframento: esta é chamada de sua *chave pública*.

A chave pública realmente condiz com seu nome. Qualquer pessoa pode obter uma cópia dela. *Bob* inclusive encoraja isto, enviando-a para seus amigos ou publicando-a em boletins. Assim, *Eve* não tem nenhuma dificuldade em obtê-la. Quando *Alice* deseja enviar uma mensagem a *Bob*, precisa primeiro encontrar a chave pública dele. Feito isto, ela cifra sua mensagem utilizando a chave pública de *Bob*, despachando-a em seguida. Quando *Bob* recebe a mensagem, ele a decifra facilmente com sua chave privada. *Eve*, que interceptou a mensagem em trânsito, não conhece a chave privada de *Bob*, embora conheça sua chave pública. Mas este conhecimento não o ajuda a decifrar a mensagem. Mesmo *Alice*, que foi quem cifrou a mensagem com a chave pública de *Bob*, não pode decifrá-la agora.

A grande vantagem deste sistema é permitir que qualquer um possa enviar uma mensagem secreta, apenas utilizando a chave pública de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio de chaves como é feito no modelo simétrico. A confidencialidade da mensagem é garantida, enquanto a chave privada estiver segura. Caso contrário, quem possuir acesso à chave privada terá acesso às mensagens.

Dentro dos Algoritmos Criptográficos de Chave Pública, o RSA é um dos mais difundidos e usados. Criado por, entre outros, Shamir, um pesquisador Israelita naturalizado americano e um dos maiores críticos do DES e dos demais algoritmos de chave única.

5.3.1 - RSA

Basicamente o RSA trabalha com números primos para a escolha das chaves. Devem ser escolhidos 2 números primos aleatoriamente e com, no mínimo, 150 digitos decimais cada um (maior do que 512 bits). Esses números primos são chamados de p e q.

O próximo passo é calcular n=pxq. Após isso é calculada uma função f(n)=(p-1)x(q-1) para então ser escolhido um número primo e em relação a função f. Ou seja, f(n) não podem ter nenhum divisor comum que não seja o número 1.

O próximo passo é o cálculo do número d. esse número deve ser calculado tal que (exd)mod f(n)=1, ou seja, d=1/e mod f(n). Feito isso já temos a chave todos os dados para a escolha das chaves. O par de números (n, e) é escolhido, por definição, como a Chave privada, e o par (n,d) é escolhido como a Chave Pública. Hyperlink reference not valid.

É importante ressaltar que a escolha inicial de 2 números primos não é 100% garantida, na verdade a garantia de que os números escolhidos (p, q) são realmente primos é de 90%.

Bom, de posse das chaves pública e privada, deve-se então partir para a cifragem e decifragem, o que não poderia ser mais simples de explicar:

Cifragem: C=(M**e) mod n

Decifragem: D=(M**d) mod n onde C significa crypt, D significa decrypt e M significa a mensagem em claro.

Dentro das técnicas de criptografia de Chave Pública, o Hyperlink reference not valid. É uma aplicação que permite a autenticação de 2 pessoas frente a um servidor de autenticação chamado de CE (Distributed Computing Environment),. Vários fornecedores como IBM, NEC, HP e Sun, planeam tornar o Kerberos parte de seus Sistemas Operativos UNIX. Vide Anexo II (Quadro de Resumo do Algorítmo RSA)

CAPÍTULO VI

6 - CRIPTOANÁLISE

6.1 - CRIPTO ANÁLISE DIFERENCIAL

Em 1990, Eli Biham e Adi Shamir, ambos israelitas, introduziram o termo differential cryptanalysis (ou, criptoanálise diferencial). Era lançado um novo método de criptoanálise através do qual Biham e Shamir mostravam uma maneira de quebrar o DES com maior eficiência do que o método da força bruta.

A criptoanálise diferencial procura por pares de textos em claro e pares de textos cifrados. Especificamente, o ataque examina os pares cifrados: pares de textos cifrados cujos textos em claro têm certas particularidades. Os dois textos em claro podem ser escolhidos randomicamente, até que se satisfaçam as tais condições particulares, e o criptoanalista não necessita saber seus valores.

Certas diferenças presentes nos pares de textos em claro têm alta probabilidade de se repetirem nos pares de textos cifrados. A isto chama-se características. Por exemplo, se a diferença entre dois de texto em claro em hexadecimal é 0080 8200 6000 000, então (ignorando a permutação inicial do DES) depois de três interações provalmente a diferença continua a mesma. Biham e Shamir encontraram várias características semelhantes. A criptoanálise usa estas caracterísiticas para aumentar as possibilidades de encontrar a possível chave ou, eventualmente, encontrar a chave. Porém este é um ataque estatístico e poderá falhar em alguns casos.

Este tipo de ataque funciona bem contra o DES ou qualquer outro tipo de algoritmo que utilize uma estrutura de caixas S semelhante a do DES.

6.1.1 - EXAUSTÃO (FORÇA BRUTA)

Pelo método de pura exaustão, aplica-se o algoritmo a um determinado texto cifrado, variando-se a chave até que seja produzido um texto em claro, descobre-se desta forma qual é a chave usada e todos os textos cifrados com ele são consequentemente decifrados. Mesmo quando o sistema de exaustão for realizada por computadores muito rápidos, o uso de um grande número de chaves inviabilizaria o processo.

6.1.2 - QUEBRA DO ALGORITMO

A "quebra do algoritmo", consiste na descoberta de brechas na sua estrutura, as quais o criptoanalista consegue explorar reduzindo a exaustão a tempos razoáveis. Um algoritmo é considerado realmente seguro quando não existe nenhuma maneira mais rápida de quebrá-lo que não seja a da exaustão ou força bruta.

Dois factores são necessários, mas não suficientes, para tornar possível o descobrimento de fraquezas nos algoritmos:

- mesmo utilizando-se sequências e aparência aleatória, os algorítmos têm comportamento determinístico;

- a linguagem a ser cifrada possui redundâncias, ou frequência de repetição das letras.

O conhecimento dos diversos sistemas de ataque a algoritmos conhecidos não invalida a afirmativa de que a criptoanálise ainda está mais para a arte do que para a ciência. Isto significa que experiência e, principalmente, intuição exercem papéis essenciais. Com sorte, um criptoanalista pode deparar com a solução numa semana, às vezes pode levar anos.

6.1.3 - ASSINATURA DIGITAL (8)

Outro benefício da criptografia com chave pública é a assinatura digital, que permite garantir a autenticidade de quem envia a mensagem, associada à integridade do seu conteúdo. Por exemplo, suponha que Alice (origem) queira comunicar o nascimento de sua filha para todos os seus amigos (destinatários = Bob), mas queira garantir aos mesmos que a mensagem foi enviada realmente por ela. E, embora não se importe com o sigilo da mensagem, deseja que a mesma chegue integra aos destinatários, sem alterações como, por exemplo, do sexo da criança.

Alice então cifra a mensagem com sua chave privada e a envia, em um processo denominado de assinatura digital. Cada um que receber a mensagem deverá decifrá-la, ou seja, verificar a validade da assinatura digital, utilizando para isso a chave pública de Alice. Como a chave pública de Alice apenas decifra (ou seja, verifica a validade de) mensagens cifradas com sua chave privada, fica garantida assim a autenticidade, integridade e não-repudiação da mensagem. Pois se alguém modificar um bit do conteúdo da mensagem ou se outra pessoa assiná-la ao invés de Alice, o sistema de verificação não irá reconhecer a assinatura digital de Alice como sendo válida.

É importante perceber que a assinatura digital, como descrita no exemplo anterior, não garante a confidencialidade da mensagem. Qualquer um poderá acessá-la e verificá-la, mesmo um intruso (*Eve*), apenas utilizando a chave pública de *Alice*. Para obter confidencialidade com assinatura digital, basta combinar os dois métodos. Alice primeiro assina a mensagem, utilizando sua chave privada. Em seguida, ela criptografa a mensagem novamente, junto com sua assinatura, utilizando a chave pública de Bob. Este, ao receber a mensagem, deve, primeiramente, decifrá-la com sua chave privada, o que garante sua privacidade. Em seguida, "decifrá-la" novamente, ou seja, verificar sua assinatura utilizando a chave pública de Alice, garantindo assim sua autenticidade.

CAPÍTULO VII

7 - SISTEMAS BIOMÉTRICOS

Nos últimos anos tem se pesquisado na área de sistemas automáticos de verificação de identidade baseados em caracterísiticas físicas do usuário. Esses estudos têm como objectivo suprir deficiências de segurança das senhas, que podem ser reveladas ou descobertas, o que é das tokens, que podem ser perdidas ou roubadas. Acredita se que esses sistemas são dificies de serem forjados, porém são bem mais caros, na sua implementação.

Seguem-se alguns sistemas utilizados:

7.1 - IMPRESSÕES DIGITAIS

São caracterísiticas únicas e consistentes. Nos sistemas biométricos que utilizam esta opção, são armazenados de 40 a 60 pontos para verificar uma identidade. O sistema compara a impressão lida com sua base de dados de impressões digitais de pessoas autorizadas.

7.1.2 - VOZ

Os sistemas de reconhecimentos de voz são usados para controle de acesso, porém não são tão confiáveis, em função dos erros causados por ruídos no ambiente e problemas na garganta ou nas cordas vocais das pessoas a ele submetidas.

7.1.3 - GEOMETRIA DA MÃO

Também é usada em sistema de controle de acesso, porém essa caracterítica pode ser alterada por aumento ou diminuição de peso.

7.1.4 - CONFIGURAÇÃO DA ÍRIS E DA RETINA

Esses sistemas se propõem a efectuar uma identificação mais confiável do que as impressões digitais. Entretanto são sistemas invasivos, pois direcionam feixes de luz para os olhos das pessoas.

7.1.5 - RECONHECIMENTO FÁCIL POR MEIO DE TERMOGRAMA

O termograma fácil é uma imagem retirada com uma câmara infravermelha que mostra padrões térmicos de uma face. Essa imagem é única e, combinada com algorítmos sofisticados de comparação de diferentes níveis de temperatura distribuídos pela face, constitui-se em técnica não invasiva, altamente confiável, não sendo afectada por alterações de saúde, idade ou temperatura do corpo. São armazenadas ao todo 19.000 pontos de identificação, podendo distinguir gêmeos idênticos, mesmo no escuro. Pesquisas estão sendo feitas na área fins baratear seus custos.

7.1.6 - USO DE SISTEMAS BIOMÉTRICOS

Depois dos ataques terroristas em Nova Iorque e Washington, a 11 de Setembro de 2001 estas tecnologias de segurança, que até então eram consideradas caras ou muito invasivas para serem usadas em aeroportos, estão agora sendo estudadas, pelas autoridades Aeroportuários pensam em usar desde verificadores de impressões digitais computadores até raios x que procuram por armas escondidas sob as roupas de passageiros tecnologias que incluem um scanner de olhos computarizado, que actualmente está sendo instalado no Aeroporto Heathrow, em Londres. Verificadores digitais já estão sendo usados para o controle de acesso de funcionários de sete aeroportos americanos, incluíndo o Logan, em Boston. Os aparelhos cruzam dados dos funcionários com um arquivo de criminosos.

Algumas linhas aéreas pretendem adotar a verificação da identidade dos passageiros através da consulta de um banco de dados com uma relação de criminosos como medida de segurança.

Abaixo se indicam os locais que usam este tipo de sistema.

Reconhecimento de identidade (cartão magnético)

- FBI
- NBS
- Cornell Aeronautical laboratory
- Rockwell International Corp
- NEC
- Printmaker Morph Systems
- ICL PLC
- Cambridje Neurodynanamics
- Orincon Cor
- Controle de acesso a áreas no Pentágono
- Acesso computadores redes financeiras na Itália
- Automated Banking Terminal na Australia
- Alfândega e imigração em Amsterdan

Mão

- San Francisco Intl Airport (controle acesso operações)
- Lótus (visitantes fora da áreas reservadas)
- University of Georgia (refeições consumidas)
- Prisão em Jessup
- Aeroporto Kenneddy e Newark (inspeção automática de passaporte e controle de pessoas que se registaram como passageiros frequentes)
- Câmara dos Deputados e Senado na Colómbia para evitar fraude nas votações

Íris

- Sul SparcStation para análise

CAPÍTULO VIII

8 - FIRE WALL

8.1 - OBJECTIVOS

Como o próprio nome sugere, um dos objectivos mais importantes de um firewall é reduzir os danos em caso de um desastre, exatamente como acontece quando há um incêndio num carro ou em um edifício. No contexto da Internet, o firewall tem uma finalidade semelhante, protegendo uma rede contra invasões vindas da Internet e regulando o fluxo do tráfego entre duas redes

Tradicionalmente, essas duas têm sido a Internet e a rede cooperativa, mas o firewall também pode ser usado entre duas redes quaisquer com diferentes necessidades de segurança.

Neste trabalhos, abordamos a utilização dos firewalls levando em conta que as possíveis invasões venham da redes das redes, ou seja, da Internet. Neste caso, os firewalls são ferramentas extremamente avançadas que oferecem segurança à rede, além de representarem uma eficiente estratégia para implementar uma política de acesso à Internet numa organização.

Os firewalls podem oferecer protecções contra ataques a protocolos ou aplicações individuais, além de possuirem relativa flexibilidade de configuração, ou seja, oferecem várias restrições para diferentes tipos de tráfego. Os firewalls implementam controle de acesso baseados nos conteúdos dos pacotes de uma conexão. A melhor maneira de entender como age um firewall é imaginá-lo como um grande guarda, ou sentinela, da rede, que inspecciona a documentação para todos os pacotes que chegam e depois decide se dará autorização para passagem ou não.

Além disso, os firewall também servem para ocultar algumas máquinas de outras. Alguns são configurados para mascarar a topologia interna de uma rede através da restrição das

divulgações do DNS e dos endereços de rede no tráfego de saída. Uma das grandes vantagens do firewall é que ele oferece um único ponto de controle para a segurança numa rede e um único ponto de administração de segurança, além de serem óptimos para auditoria e monitoração da rede.

Porém como toda a segurança da rede é concebida pelo firewall, se o invasor conseguir "quebrar"o firewall todo o perímetro seguro será violado e o intruso terá acesso livre a toda rede da cooperação

8.2 - LIMITAÇÕES DOS FIREWALLS

Os firewalls não representam uma cura definitiva para todos os males da segurança na Internet. Há várias tarefas que os firewalles não são capazes de executar, como por exemplo:

8.3 - INTEGRIDADE DOS DADOS

8.3.1 - AUTENDICIDADE DA ORIGEM DOS DADOS:

O firewall não tem controle sobre como o pacote foi criado, ou o que ele faz quando chega a seu destino. Um problema de segurança com o TCP/TP é que qualquer um pode gerar uma mensagem se fazendo passar por outra máquina (chamado ataque de Spoofing).

8.3.2 - SÍGILO DOS DADOS:

Apesar de alguns fornecedores de firewall actualmente permitirem o tráfego criptografado entre dois firewall, isso exige que todas as pessoas que se comunicam com consigo tenham o mesmo firewall instalado. Além disso o firewall não garante qualquer privacidade para os dados da rede interna.

8.3.3 - PROTECÇÃO CONTRA AMEAÇAS INTERNAS:

Um bom firewall pode e deve proteger você contra quase todos ataques externos baseados na Internet, mas nada faz contra ataques internos.

Um firewall não oferece segurança para um tráfego que não passe por ele.

8.3.4 - TÉCNICAS USADAS

No geral, as empresas utilizam três tipos de firewall:

- Filtros de pacotes
- Filtros Intelegentes
- Gateways de Aplicação

8.3.5 - FILTROS DE PACOTES

Talvez esta seja a maneira mais fácil e mais barata de se implementar um firewall, seja no roteador que conecta a rede privada à Internet. Como de qualquer forma você deve ter um roteador na conexão, faz sentido usar a capacidade de filtragem do roteador para implementar a segurança. De facto, até alguns anos atrás, era assim que os firewalls eram implementados.

Apesar de originalmente terem sido projetados para controlar a largura de banda em ligações muito utilizadas, os filtros de pacotes baseados no roteador oferecem uma razoável funcionalidade em termos de segurança, com o tempo, foram reconhecidos como uma importante ferramenta de segurança. Até hoje uma grande razão para sua popularidade é a incrível transparência com que os filtros baseados no roteador funcionam. A maioria dos filtros podem ser implementadas sem a menor inconviniência para o usuário final, que as vezes nem fica sabendo de sua existência.

Entretanto, a filtragem dos pacotes não se limita aos roteadores. Existem diversos filtros baseados em hosts disponíveis e domínio público.

O princípio básico por detrás dos filtros de pacotes é simples. Com base na tecnologia "store-and forward" (armazenamento e encaminhamento) dos roteadores, um roteador ou um host receberá um pacote numa interface, comparará as informações no seu cabeçalho com um conjunto de filtros e então decidirá se deixa o pacote passar. Caso o rejeite ou o abandone, uma mensagem IGPM será enviada ao emissor avisando que o pacote foi abandonado.

A maioria dos filtros de pacotes levam em consideração os seguintes critérios:

- A direcção do tráfego.
- A interface na qual o tráfego foi recebido ou para qual se destina..
- O tipo de protocolo.
- Os endereços IP de origem e de destino.
- A porta TCP ou UDP de origem e de destino.
- Informações sobre o estado TCP.

8.3.6 - LIMITAÇÕES DOS FILTROS

Os filtros de pacotes, entretanto, têm algumas limitações inerentes.

Imagine uma empresa que deseja controlar o acesso proviniente da Internet, mas quer que seus funcionários utilizem a Internet à vontade. Essa empresa pode, com facilidade, bloquear o tráfego destinado aos servidores internos telnet, Email, www, ftp, etc. Entretanto se a empresa fosse bloquear todo o tráfego recebido em todas as portas das máquinas internas, o tráfego de retorno para as solicitações estaria bloqueado assim como as conexões não autorizadas. Uma vez que a empresa chegue a conclusão de que todo tráfego de retorno se destina as portas acima de 1024, a saída seria bloquear todas as portas privilegiadas, que são as portas utilizadas pelos serviços mais conhecidos da Internet, e autorizar as portas não privilegiadas. No entanto ao abrir todas as portas não privilegiadas, a empresa permite não só que os servidores externos

respondam a solicitações de clientes, mas também que clientes externos estabeçam conexões com servidores internos que por acaso estejam sendo executadas em portas de numeração alta

8.3.7 - PROBLEMAS

Incapacidade de manter um log do tráfego: sem um tipo qualquer de log de pacote, é muito difícil assegurar a integridade do firewall e determinar os padões de uso da Internet para reavaliar decisões políticas em relação a protocolos específicos.

Incapacidade de autenticação do usuário: Como não poderia deixar de ser, qualquer forma de autenticação, como o uso de senhas por exemplo, é vista como um requisito fundamental para a segurança.

- Falta de ferramentas para administração.

8.3.8 - FILTROS INTELIGENTES

São filtros baseados em hosts que desempenham as mesmas funções gerais que os filtros de pacotes desempenham, mas que têm maior funcionalidade e não apresentam parte dos problemas associados aos filtros de pacotes.

A maioria dos filtros inteligentes possui uma interface GUI administrativa para facilitar a configuração dos filtros de pacotes. Os filtros intelegentes podem fazer log dos pacotes e usam algum recurso heurístico para verificação de regras afim de assegurar que as regras de uma lista de acesso não sejam conflitantes.

Alguns filtros inteligentes resolvem também o problema da limitação dos filtros de pacotes, além de aceitarem autenticação nas conexões.

Como podemos perceber, os filtros inteligentes são na verdade uma grande melhoria corelação aos filtros de pacotes.

8.3.9 - GATEWAY DE APLICAÇÃO

A idéia central é colocar uma espécie de portão entre as aplicações e as solicitações, deixando para o firewall apenas realizar a filtragem de pacotes. Para isso podemos usar um servidor proxy.

8.3.10 - SERVIDOR PROXY

O servidor proxy (procuração) ao receber uma conexão, a encerra e inicia uma segunda conexão para o destino. Em geral, os servidores proxy têm várias interfaces de rede, o que permite que eles se comuniquem com várias redes. Por essa razão, as máquinas nas quais o servidor proxy é configurado são quase sempre chamadas de gateways de base dupla.

8.3.11 - GATEWAY DE BASE DUPLA

Um gateway de base dupla pertence a duas redes e funciona como um ponto regular entre elas.

Para estabelecer uma conexão com as duas redes, o usuário teria que fazer um login com o gateway para depois estabelecer conexão com o destino. Ou seja, o usuário teria que ter contas em todos os destinos que quisesse fazer uma conexão. Esta abordagem tem um grande número de problemas. Para começar, ela é uma dor de cabeça. A maioria dos usuários não tem paciência para fazer vários logins em várias máquinas, nem quer memorizar mais uma senha.

Depois disso cada usuário deve ter algum tipo de shell para a máquina do gateway.

8.3.12 - SERVIDOR PROXY DE APLICAÇÃO

Os servidores proxy enriquecem muito o gateway de base dupla. Apesar de o conceito geral de "store-and-forward" ainda fazer sentido, o servidor proxy facilita a vida do usuário, pois estabelece a segunda conexão com a máquina remota para o usuário.

Os servidores proxy também evitam a necessidade de o usuário acessar o sistema operacional no firewall.

A principal vantagem do servidor proxy, porém, é que ao contrário dos filtros de pacotes, eles escondem o host interno do servidor destino. Para empresas que não desejam que sua rede interna seja visível ao mundo exterior, essa é uma grande vantagem.

Em geral existem três tipos de servidores proxy;

- Servidores proxy de aplicação específica.
- Proxys de aplicação genética.
- Servidores proxy de circuito.

8.4 - RESUMO DAS TÉCNICAS

Filtros de Pacotes

Completamente transparentes.

- Disponível no hardware existente.
- Baixo custo.
- Dificuldade para administrar.

Difícil de configurar.

Não faz log.

Não autentica usuários.

Dificulta a ocultação da estrutura interna

8.4.1 - FILTROS INTELIGENTES

- Fáceis de configurar
- Resolvem alguns problemas dos filtros de pacotes.
- Completamente transparentes.

Dificulta a ocultação da estrutura interna

Ocultam totalmente a rede

Alto nível de controle sobre o acesso do usuário.

Incovinientes para o usuário final.

Exigem mudanças no comportamento do usuário.

Necessidade de vários proxyes.

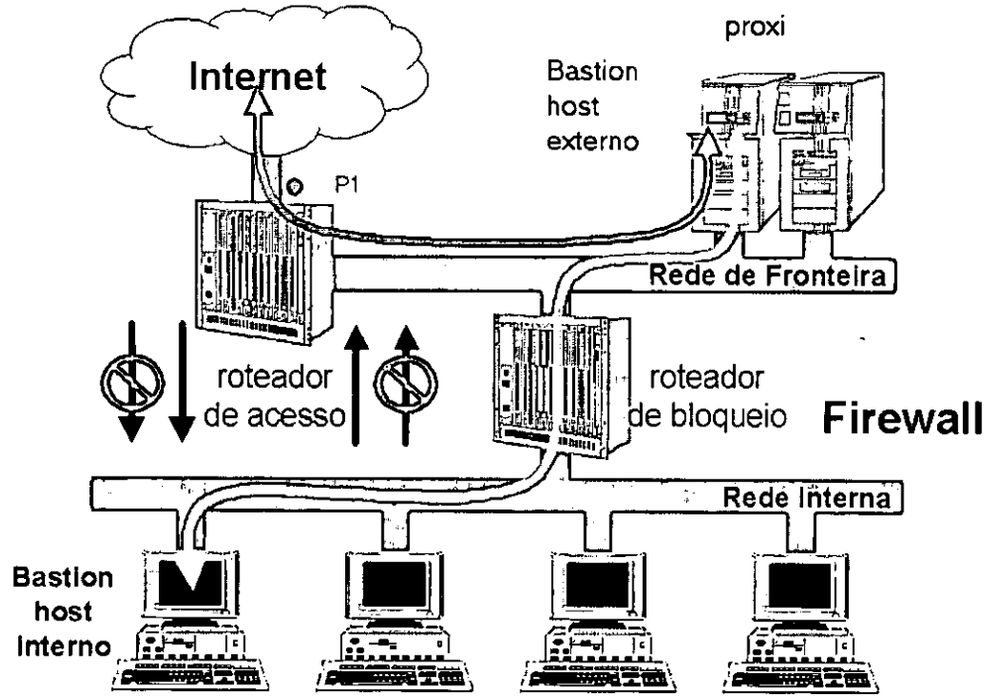
Custo elevado.

CAPÍTULO IX

9 - ARQUITETURA DOS FIREWALL MAIS USADA

A maioria das empresas preferem implementar um firewall baseado em apenas uma máquina, seja ela um host ou um roteador. Com frequência os firewalls mais rigorosos são compostos de várias partes.

Dando continuidade a análise em causa iremos descrever a figura a baixo.



9.1 - FUNÇÃO DA REDE DE FRONTEIRA

A função é acrescentar um novo nível de segurança na arquitetura de Firewall. Caso o Bastion Host externo sejam comprometido, há ainda mais um nível de segurança a ser superado. A Rede de Fronteira é tipicamente baseado em dois Roteadores: Roteador de Acesso conectando a Rede de Fronteira a Internet, Roteador de Bloqueio ligando a Rede de Fronteira a rede interna.

9.2 - FUNÇÃO DOS ROTEADORES DE ACESSO E DE BLOQUEIO

O roteador de acesso protege a rede interna e a rede de fronteira da Internet, sendo o único mecanismo de protecção complementar da rede de fronteira. O roteador de bloqueio protege a rede da Internet e da rede de fronteira limitando o acesso ao bastion host e hosts internos.

Obs: O fabricante de cada um dos roteadores deverá ser diferente afim de dificultar um hacker que conheça um bug de um dos roteadores.

9.3 - FUNÇÃO DO BASTION HOST INTERNO

Permite que hosts internos abram conexões com a Internet para serviços permitidos, inibe todas as outras conexões de/para hosts internos.

9.3.1 - FUNÇÃO DO PROXI OU BASTION HOST EXTERNO

Os pacotes externos são filtrados para as portas do bastion host da rede de fronteira pelo roteador de acesso, o roteador de bloqueio faz o mesmo para os pacotes internos.

Para ser mais claro, a função do bastion host e proxi aqui é disponibilizar para o público internet aplicações da rede interna que não seria seguro ser feito dentro da rede interna.

Uma outra função é fazer que a comunicação dos hosts internos com a internet seja feita a partir deles, impedindo que endereços Ips internos sejam vistos pela internet.

CAPÍTULO X

10 - SENHAS DE SEGURANÇA

Na área de informática existe um axioma que afirma que se os usuários costumam compartilhar senhas, não há tecnologia no mundo capaz de proteger seus sistemas.

A necessidade de uma boa senha, no ambiente de informática é a ferramenta de maior importância, uma boa senha é capaz de garantir 90% de segurança de seus sistemas.

Assim importa ter numa senha características de boas senhas e más senhas sendo boa senha que não seja facilmente decifrável.

Características de boas senhas

- Devem ter caracteres maiúsculos e minúsculos.
- Dígitos e/ou caracteres de pontuação.
- Fáceis de lembrar.
- Ter no mínimo 7 caracteres.

Características de más senhas

- São aquelas fáceis de descobrir:
- Baseadas em informações
- Com poucos dígitos
- Usam nomes próprios.
- Palavras em qualquer língua
- Combinações de teclado (qwerty)

10.1 - ALGUMAS INFORMAÇÕES DE AUDITORIA DEVEM SER FORNECIDAS DIRECTAMENTE AOS USUÁRIOS:

- Data e hora do último acesso.
- Data e hora do último acesso mal sucedido.

Mudanças regulares de senhas.

Data de expiração e a sua renovação períodica.

Impor regras rígidas de formação de senha.

Não impor regras extremamente rígidas, senão os usuários anotarão a senha no papel

Tentar quebrar suas próprias senhas.

Não usar a mesma senha em ambientes distintos.

Remover senhas inativas.

10.2 - SENHAS AVANÇADAS

A tecnologia conhecida como one-time password ou Tecnologia S/KEY visa mudar a cada minuto a senha de acesso. A cada conexão é necessária uma nova senha. Visa proteger contra ataques de escuta, as senhas que trafegam criptografadas por algorítimo irreversível (MD4), não protege contra ataques de dicionário.

A tecnologia SecurID gera novas senhas a cada 60 segundos, cada dispositivo possui uma identificação própria que permite que o mesmo seja bloqueado em caso de furto ou roubo, imune a ataques de dicionário, a seu é custo elevado.

10.3 - OUTRAS OPÇÕES

Como os usuários podem resistir ao uso da s/key ou SecurID existe uma opção: O Secure Shell (SSH) que fornece comunicações seguras num ambiente de aplicações Telnet. O SSH é um exemplo perfeito de um aplicativo que atende aos padrões do usúario e administrativos. Esta é uma forma de derrotar Sniffer na rede.

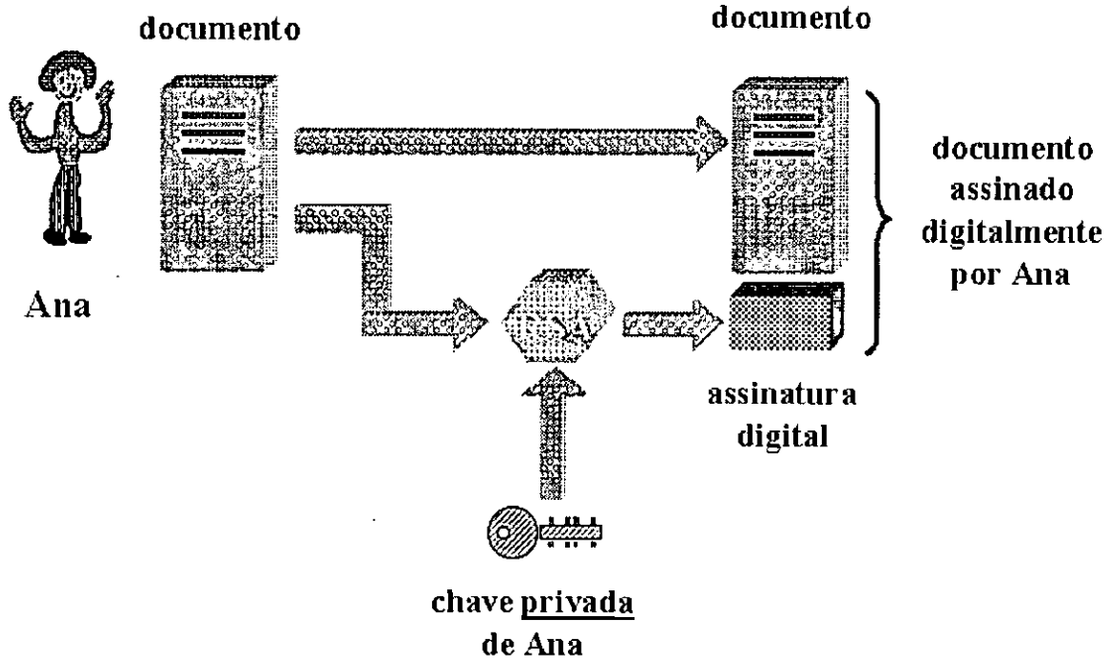
10.4 - GERENCIADORES DE SENHA

A profusão de senhas na Internet e a dificuldade de lembrá-las e armazená-las com segurança abriram espaço para o surgimento de um novo tipo de aplicativo: o gerenciador de senhas. A maioria deles consiste em banco de dados para coleccionar senhas, em geral dotados de algum tipo de protecção.

Os maiores destaques nesta categoria são os aplicativos que combinam o gerenciamento de senhas com navegação na Internet.

Os dois títulos mais destacados nesta área são: O Gator ambos tem versões gratuitas. Há ainda um novo produto brasileiro. O did que opera de forma semelhante ao gator.

Obs: O Gator é mais indicado para senhas nos passeios pela internet já o Quallet é licenciado para cartões de crédito e instituições financeiras, o Did se assemelha com o Qwallet em termos de protecção e segurança de dados.



Segue a descrição de alguns algoritmos utilizados para assinatura digital no anexo III.

CAPÍTULO IV

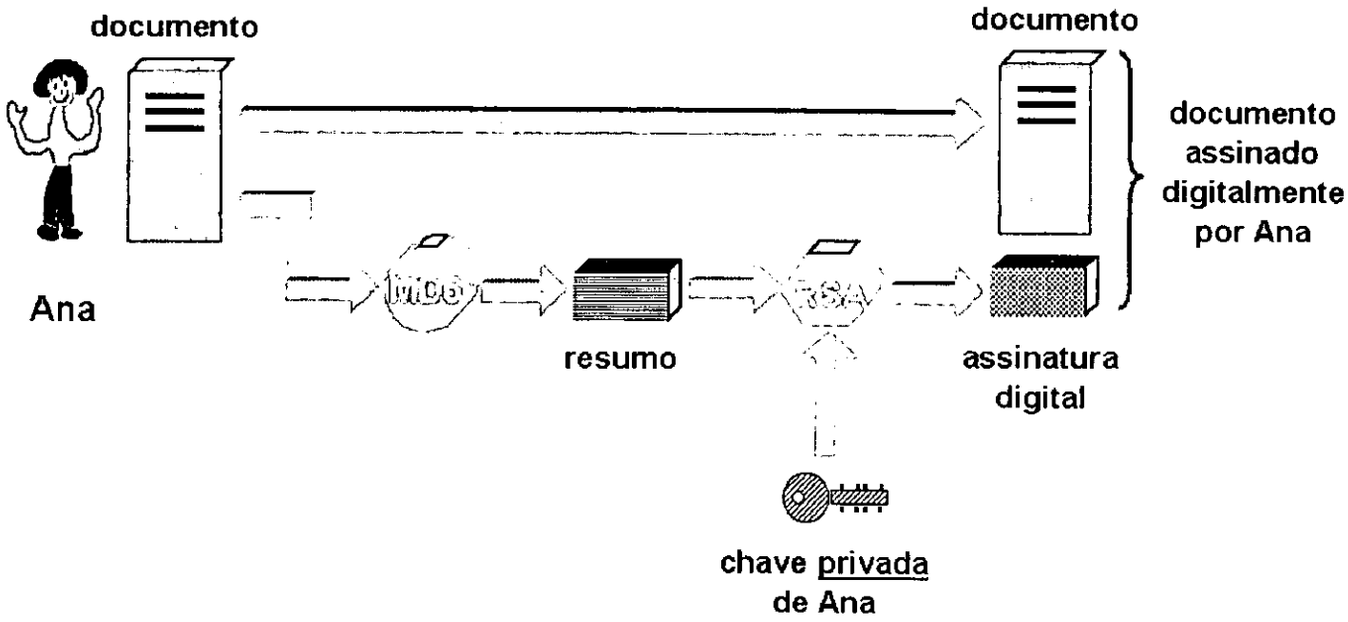
11 - FUNÇÃO HASHING

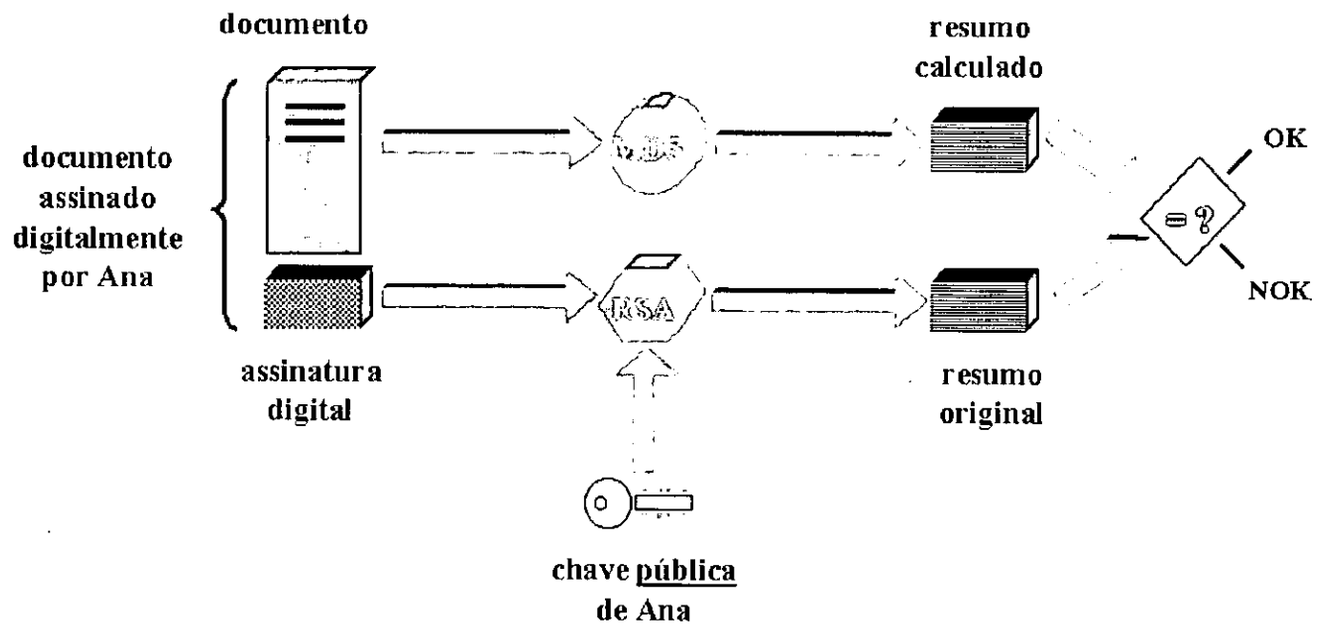
A assinatura digital obtida através do uso da criptografia assimétrica ou de chave pública infelizmente não pode ser empregada, na prática, de forma isolada, do modo como foi didaticamente descrito no item anterior. Está faltando, portanto, descrever um mecanismo fundamental para o adequado emprego da assinatura digital. Este mecanismo é a função Hashing. Sua utilização como componente de assinaturas digitais se faz necessário devido à lentidão dos algoritmos assimétricos, em geral cerca de 1.000 vezes mais lentos do que os simétricos.

Assim, na prática é inviável e contraproducente utilizar puramente algoritmos de chave pública para assinaturas digitais, principalmente quando se deseja assinar grandes mensagens, que podem levar preciosos minutos ou mesmo horas para serem integralmente "cifradas" com a chave privada de alguém. Ao invés disso, é empregada uma função Hashing, que gera um valor pequeno, de tamanho fixo, derivado da mensagem que se pretende assinar, de qualquer tamanho. Assim, a função Hashing oferece agilidade nas assinaturas digitais, além de integridade confiável, conforme descrito a seguir.

A denominada "Message Digest, One-Way Hash Function", Função de Condensação ou Função de Espalhamento Unidirecional, a função Hashing funciona como uma impressão digital de uma mensagem gerando, a partir de uma entrada de tamanho variável, um valor fixo pequeno:

Este valor está para o conteúdo da mensagem assim como o dígito verificador de uma conta-corrente está para o número da conta ou o check sum está para os valores que valida. Serve, portanto, para garantir a integridade do conteúdo da mensagem que representa. Assim, após o valor hash de uma mensagem ter sido calculado através do emprego de uma função hashing, qualquer modificação no seu conteúdo -mesmo em apenas um bit da mensagem - será detectada, pois um novo cálculo do valor hash sobre o conteúdo modificado resultará em um valor hash bastante distinto.





Segue a descrição de algumas funcões Hashing empregadas em produtos e protocolos criptográficos: Vide Anexo IV

Modelo Criptográfico Híbrido.

Qual o modelo de criptografia que devemos utilizar? Simétrico ou assimétrico? A resposta é simples: devemos utilizar os dois, num modelo denominado híbrido. O algoritmo simétrico, por ser muito mais rápido, é utilizado no ciframento da mensagem em si. Enquanto o assimétrico, embora lento, permite implementar a distribuição de chaves e a assinatura digital. Além disso, como já exposto no item anterior, deve-se utilizar também o mecanismo de Hashing para complemento da assinatura digital.

Tabela Resumo dos dois métodos criptográficos vistos anteriormente

Criptografia Simétrica.	Criptografia Assimétrica.
Rápida.	Lenta.
Gerência e distribuição das chaves é complexa.	Gerência e distribuição simples.
Não oferece assinatura digital	Oferece assinatura digital.

Em resumo, os algoritmos criptográficos podem ser combinados para a implementação dos três mecanismos criptográficos básicos: o ciframento, a assinatura e o Hashing. Estes mecanismos são componentes dos protocolos criptográficos, embutidos na arquitetura de segurança dos produtos destinados ao comércio electrônico. Estes protocolos criptográficos, portanto, provêm os serviços associados à criptografia que viabilizam o comércio electrônico: que são disponibilidade, sigilo, controle de acesso, autenticidade, integridade e não-repúdio.

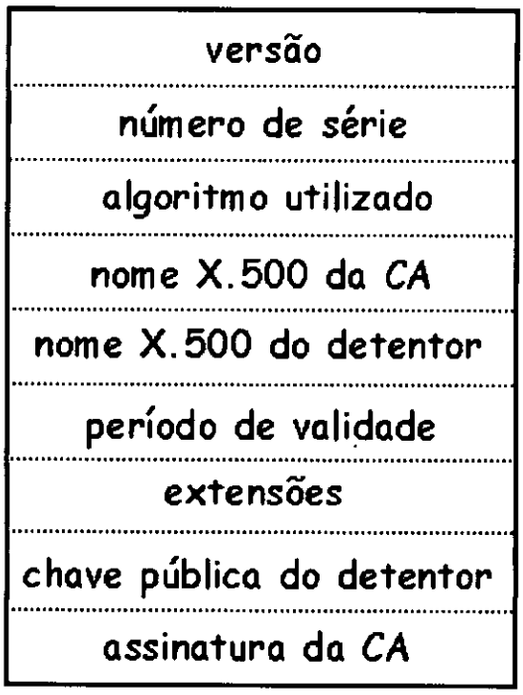
Seguem exemplos de protocolos que empregam sistemas criptográficos híbridos: Vide Anexo V

CERTIFICADO DIGITAL

Com um sistema de chave pública, o gerenciamento de chaves passa a ter dois novos aspectos: primeiro, deve-se previamente localizar a chave pública de qualquer pessoa com quem se deseja comunicar e, segundo, deve-se obter uma garantia de que a chave pública encontrada seja proveniente daquela pessoa (*Bob*). Sem esta garantia, um intruso *Eve* pode convencer os interlocutores (*Alice* e *Bob*) de que chaves públicas falsas pertencem a eles. Estabelecendo um processo de confiança entre os interlocutores, *Eve* pode fazer-se passar por ambos.

Deste modo, quando um interlocutor (*Alice*) enviar uma mensagem ao outro (*Bob*) solicitando sua chave pública, o intruso poderá interceptá-la e devolver-lhe uma chave pública forjada por ele. Ele também pode fazer o mesmo com o recebedor (*Bob*), fazendo com que cada lado pense que está se comunicando com o outro, quando na verdade estão sendo interceptados pelo intruso. *Eve* então pode decifrar todas as mensagens, cifrá-las novamente ou, se preferir, pode até substituí-las por outras mensagens. Através deste ataque, um intruso pode causar tantos danos ou até mais do que causaria se conseguisse quebrar o algoritmo de ciframento empregado pelos interlocutores.

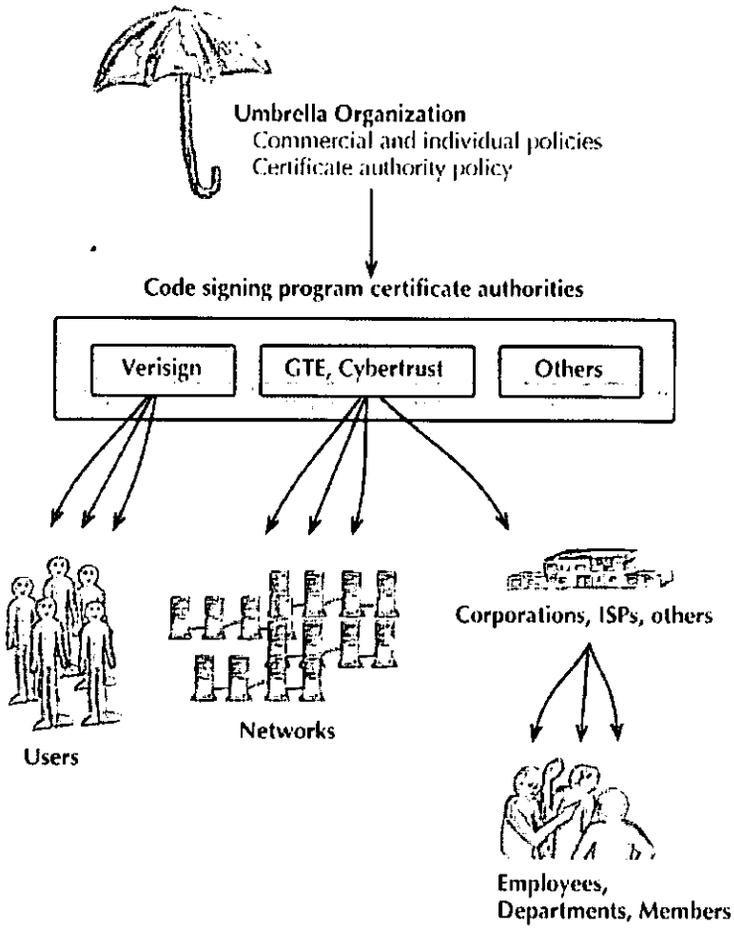
A garantia para evitar este ataque é representada pelos *certificados de chave pública*. Tais certificados consistem em chaves públicas assinadas por uma pessoa de confiança, geralmente no formato padrão ITU X.509v3. Servem para evitar tentativas de substituição de uma chave pública por outra. O certificado de *Bob* contém algo mais do que sua chave pública: contém informações sobre *Bob* - seu nome, endereço e outras dados pessoais - e é assinado por alguém em quem *Alice* deposita sua confiança: uma *autoridade de certificação* ou *CA* (*Certification Authority*), que funciona como um cartório electrônico.



Assim, um certificado digital pode ser definido como um documento electrônico, assinado digitalmente por uma terceira parte confiável, que associa o nome (e atributos) de uma pessoa ou instituição a uma chave criptográfica pública.

Pela assinatura da chave pública e das informações sobre *Bob*, a CA garante que a informação sobre *Bob* está correcta e que a chave pública em questão realmente pertence a *Bob*. *Alice*, por sua vez, confere a assinatura da CA e então utiliza a chave pública em pauta, segura de que esta pertence a *Bob* e a ninguém mais. Certificados desempenham um importante papel em um grande número de protocolos e padrões utilizados na protecção de sistemas de comércio electrônico.

Autoridades de certificação, como Verisign, Cybertrust e Nortel, assinam certificados digitais garantindo sua validade. Uma CA também tem a responsabilidade de manter e divulgar uma lista com os certificados revogados (Certificate Revocation List - CRL). Certificados nesta lista podem ter sido roubados, perdidos ou, simplesmente, estar sem utilidade. As CAs podem estar encadeadas em hierarquias de certificação, onde a CA de um nível inferior válida sua assinatura com a assinatura de uma CA mais alta na hierarquia.



Existem diversos tipos de cerificados, conforme descrição feita a seguir.

Certificados de CA: utilizados para validar outros certificados; são auto-assinados ou assinados por outra CA.

Certificados de servidor: utilizados para identificar um servidor seguro; contém o nome da organização e o nome DNS do servidor.

Certificados pessoais: contém nome do portador e, eventualmente, informações como endereço electrônico, endereço postal, etc.

Certificados de desenvolvedores de software: utilizados para validar assinaturas associadas a programas.

A infra-estrutura para lidar com o gerenciamento de chaves públicas é definido pelo padrão Public Key Infrastructure (PKI), que define onde os certificados digitais serão armazenados e recuperados, de que forma estão armazenados, como um certificado é revogado, entre outras informações.

CAPÍTULO XII

12 - USO DOS CÓDIGOS COM BASE IRRACIONAL NA SEGURANÇA DA INFORMAÇÃO

A maioria dos computadores experimentais concebidos usam o sistemas de numeração com base irracional e não os tradicionais sistemas binários, octal, hexadecimal etc. O uso deste código permitiu garantir uma melhoria substancial da segurança na transmissão de informações digitais em longas distâncias. No geral, o uso de códigos de base irracional permite detectar e corrigir erros, melhor que no sistema binário.

Comecemos por dizer que qualquer tipo de mensagem que deve ser transmitida pode ser representada no sistema binário como uma matriz que contém N-linhas, onde cada linha repesenta um vector binário que codifica um caracter desta mensagem conforme se ilustra abaixo.

Matriz inicial das combinações codificadas.

1	1	1	1	0	0	0	1
1	1	1	1	0	0	1	0
1	1	1	1	0	0	1	1
0	0	0	0	1	0	1	1

Esta matriz inicial é transmitida linha por linha até o receptor.

|.....|11111001|11110010|11110001|

N 3 2 1

Tempo

Contudo podemos também usar os codigos irracionais que oferecem igual possibilidade de trasmissão da informação digital. Assim a Matriz acima pode ser representada como:

$F_i = \| M_P \|$ onde P - Parametro do código irracional.

F_i = Mensagem codificada no código de base irracional

A Semelhança do sistema binário podemos transmitir a mensagem codificada no código de base irracional como forma de proteger a informação segundo a equação

$$\overline{F_i} = \| M_P \|$$

Onde M_P = um vector binário invertido no código de base irracional.

Como no sistema binário podemos transmitir essa matriz directamente e inversamente por isso obteremos.

$$\overleftarrow{Fi} = \| M_P \| \|$$

$$\overleftarrow{\overline{Fi}} = \| M_P \|$$

Onde M_P – vector transmitido inversamente:

$\overleftarrow{\overline{\quad}}$ M_P vector invertido na transmissão inversa

Com as matrizes estabelece-se o nível de protecção da informação a ser transmitido através do canal da rádio. Para aumentar o nível de protecção o transmissor e o receptor mudam ciclicamente a frequência de trabalho.

Na verdade são usadas no máximo três frequências o que torna a parte do hardware extremamente complexa com quatro matrizes e três frequências diferentes garante-se o máximo de protecção da informação. Do ponto de vista técnico o processo de sincronização das alterações das frequências torna-se quase que impossível dado que existem outros factores adversos tais como interferências, ruídos, variações climaticas que dificultam as recepções das informações. Uma da maneiras de minorar estes efeitos seria o uso de uma única frequência o que garante uma transmissão mais segura, mas em contrapartida diminuiria o nível de protecção N isto porque N so deve ter as variáveis o I, D

$$N \; E \; \{ I, D, F \}$$

Onde: N - nível de protecção

I - Forma da matriz inicial (normalmente invertida)

D - Direcção de transmissão (directa, indirecta)

F - O conjunto das frequências.

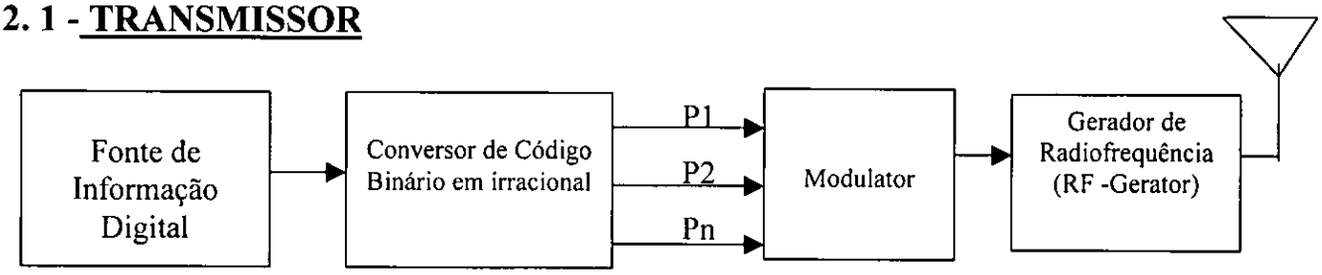
É sabido que os códigos com a base irracional podem ter vários parâmetros p = 1; p = 2; p = 3; ... Pn=n que formam os códigos posicionais, por isso podemos escrever a fórmula acima em conformidade com P.

$N \in \{I, D, P\}$

Onde: P - parâmetro do código, com base irracional.

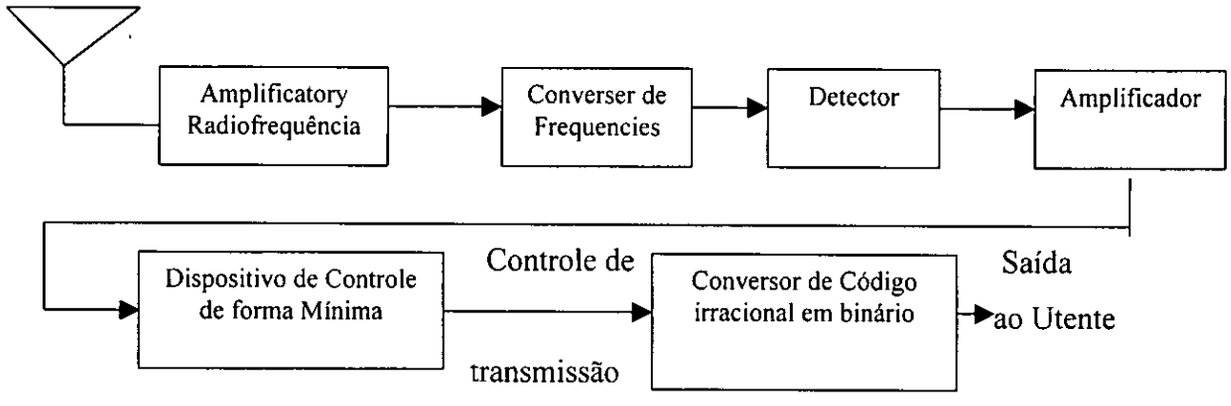
A figura abaixo ilustra o diagrama de um transmissor usado para a transmissão da informação digital.

12. 1 - TRANSMISSOR



12.2 - RADIORECEPTOR

Como podemos ver na figura abaixo um novo bloco foi introduzido que é o dispositivo de controle da forma mínima.



O seu uso aumento as possibilidades funcionais do sistema de transmissão - recepção. Se durante a transmissão da informação através do canal da Rádio surgirem erros isso irá provocar a partida alterações na forma mínima pelo menos num vector binário, o que de conformidade com as regras da forma mínima facilmente se determinará o erro e como consequência desta situação obter-se a saída do controle de tramissão um sinal lógico que informará sobre a qualidade de tramissão.

Como tudo que foi dito sobre os códigos com base irracional temos que eles permitem:

a) Transmitir a informação com alto nível de protecção.
b) Diminuir a complexidade dos dispositivos radioelectrónicos e em geral todo o sistema de transmissão e recepção de informações

3 - Determinação fácil dos erros que surgem durante a transmissão no canal de rádio.

CONCLUSÕES

Durante os últimos anos houve uma mudança crescente com relação à informática e à utilização dos seus sistemas, houve um "downsizing"destes, e a migração dos sistemas de grande porte e centralizados e automáticos para os de pequeno porte. Esta nova arquitectura denominada de cliente/servidor favoreceu a profiferação de sistemas distribuídos com compartilhamento de recursos, a rede de computadores.

Inicialmente local a rede de computadores logo cedeu lugar também para as redes de longa distância que conectava dois ou mais locais. Este advento deu origem ao crescimento da Internet, uma das grandes responsáveis pelo fenômeno da globalização.

Com a Internet e mudanças de hábitos sociais, passamos a transferir a vida do quotidiano para uma vida digital, portanto a partir daí precisamos ter todos os cuidados que temos enquanto cidadãos e usuários de serviços público e/ou privados, dos quais fazemos utilização através desta grande teia que é a Internet, neste grande e pequeno mundo da globalização.

Dentre as precauções que devemos tomar neste mundo digitalizado, está a segurança dos dados que transmitimos ou recebemos pela Rede, tendo enconta o crescente indice do terrorismo informático.

A segurança digital a que nos referimos deve estar baseada em todo um conjunto de procedimentos que devem ser rigorosamente obedecidos, que denominaremos de política de segurança, que a partir de agora fará parte do preconceito básico, isto é toda medida de segurança não será nem deverá ser vista como um procedimento isolado, mas como um fragmento de um conjunto delas, a terminar gostaria de enfatizar que a segurança é uma questão a que se deve dar alta prioridade, o que foi aquí apresentado representa alguns ítens que se devem ter em mente ao se averiguar e planear a introdução de mecanismos de segurança numa organização. Também é bom salientar que o único sistema de computação totalmente seguro é aquele que nunca foi ligado a corrente eléctrica (nunca funcionou). Cada organização deve seleccionar um nível de segurança que considere apropriado avaliado o impacto financeiro e a sua reputação no caso de um possível ataque bem sucedido ao seu site. Este trabalho pretende servir de ajuda e de incentivo na buscar de uma infraestrutura apropriada de segurança para uma organização.

ANEXOS

ANEXO I

QUADRO DE RESUMO DO ALGORITMO SIMÉTRICO

Algoritmo Simétrico	Bits	Descrição
DES	56	O Data Encryption Standard (DES) é o algoritmo simétrico mais disseminado no mundo. Foi criado pela IBM em 1977 e, apesar de permitir cerca de 72 quadrilhões de combinações (2^{56}), seu tamanho de chave (56 bits) é considerado pequeno, tendo sido quebrado por "força bruta" em 1997 em um desafio lançado na Internet. O NIST (National Institute of Standards and Technology), que lançou o desafio mencionado, recertificou o DES pela última vez em 1993 e desde então está recomendando o 3DES. O NIST está também propondo um substituto ao DES que deve aceitar chaves de 128, 192 e 256 bits, operar com blocos de 128 bits, ser eficiente, flexível e estar livre de "royalties". O novo padrão, denominado AES (Advanced Encryption Standard), está sendo estudado desde 1997 a partir de vários algoritmos apresentados pela comunidade. Os finalistas são: Serpent, Mars, RC6, Twofish e Rinjdael, e o resultado deverá ser divulgado no final de 2000.
Triple DES	112 ou 168	O 3DES é uma simples variação do DES, utilizando-o em três ciframentos suscessivos, podendo empregar uma versão com duas ou com três chaves diferentes. É seguro, porém muito lento para ser um algoritmo padrão.
IDEA	128	O International Data Encryption Algorithm foi criado em 1991 por James Massey e Xuejia Lai e possui patente da suiça ASCOM Systec. O algoritmo é estruturado seguindo as mesmas linhas gerais do DES. Mas na maioria dos microprocessadores, uma implementação por *sofiware* do IDEA é mais rápida do que uma implementação por *software* do DES. O IDEA é utilizado principalmente no mercado financeiro e no PGP, o programa para criptografia de e-mail pessoal mais disseminado no mundo.
Blowfish	32 a 448	Algoritmo desenvolvido por Bruce Schneier, que oferece a escolha entre maior segurança ou desempenho através de chaves de tamanho variável. O autor aperfeiçou-o no Twofish, concorrente ao AES.
RC2	8 a 1024	Projetado por Ron Rivest (o R da empresa RSA Data Security Inc.) e utilizado no protocolo S/MIME, voltado para criptografia de e-mail corporativo. Também possui chave de tamanho variável. Rivest também é o autor do RC4, RC5 e RC6, este último concorrente ao AES.

ANEXOS II
QUADRO RESUMO DO ALGORÍTMO RSA

Algoritmo	Descrição
RSA	O RSA é um algoritmo assimétrico que possui este nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. É, atualmente, o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. O RSA utiliza números primos. A premissa por trás do RSA é que é fácil multiplicar dois números primos para obter um terceiro número, mas muito difícil recuperar os dois primos a partir daquele terceiro número. Isto é conhecido como *factorização.* Por exemplo, os fatores primos de 3.337 são 47 e 71. Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto. Derivar a chave privada a partir da chave pública envolve fatorar um grande número. Se o número for grande o suficiente e bem escolhido, então ninguém pode fazer isto em uma quantidade de tempo razoável. Assim, a segurança do RSA baseia-se na dificuldade de factorização de números grandes. Deste modo, a factorização representa um limite superior do tempo necessário para quebrar o algoritmo. Uma chave RSA de 512 bits foi quebrada em 1999 pelo Instituto Nacional de Pesquisa da Holanda, com o apoio de cientistas de mais 6 países. Levou cerca de 7 meses e foram utilizadas 300 estações de trabalho para a quebra. Um fato preocupante: cerca de 95% dos sites de comércio eletrônico utilizam chaves RSA de 512 bits.
ElGamal	O ElGamal é outro algoritmo de chave pública utilizado para gerenciamento de chaves. Sua matemática difere da utilizada no RSA, mas também é um sistema comutativo. O algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto. Assim, o ElGamal obtém sua segurança da dificuldade de se calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da factorização.
Diffie-Hellman	Também baseado no problema do logaritmo discreto, é o criptosistema de chave pública mais antigo ainda em uso. O conceito de chave pública aliás foi introduzido pelos autores deste criptosistema em 1976. Contudo, ele não permite nem ciframento nem assinatura digital. O sistema foi projetado para permitir a dois indivíduos teclado entrarem num acordo ao compartilharem um segredo tal como uma chave, muito embora eles somente troquem mensagens em público.
Curvas Elípticas	Em 1985, Neal Koblitz e V. S. Miller propuseram de forma independente a utilização de curvas elípticas para sistemas criptográficos de chave pública. Eles não chegaram a inventar um novo algoritmo criptográfico com curvas elípticas sobre corpos finitos, mas implementaram algoritmos de chave pública já existentes, como o algoritmo de Diffie e Hellman, usando curvas elípticas. Assim, os sistemas criptográficos de curvas elípticas consistem em modificações de outros sistemas (o ElGamal, por exemplo), que passam a trabalhar no domínio das curvas elípticas, em vez de trabalharem no domínio dos corpos finitos. Eles possuem o potencial de proverem sistemas criptográficos de chave pública mais seguros, com chaves de menor tamanho. Muitos algoritmos de chave pública, como o Diffie - Hellman, o ElGamal e o Schnorr podem ser implementados em curvas elípticas sobre corpos finitos. Assim, fica resolvido um dos maiores problemas dos algoritmos de chave pública: o grande tamanho de suas chaves. Porém, os algoritmos de curvas elípticas actuais, embora possuam o potencial de serem rápidos, são em geral mais demorados do que o RSA.

ANEXO III

Algoritmo	Descrição
RSA	Como já mencionado, o RSA também é comutativo e pode ser utilizado para a geração de assinatura digital. A matemática é a mesma: há uma chave pública e uma chave privada, e a segurança do sistema baseia-se na dificuldade da factorização de números grandes.
ElGamal	Como o RSA, o ElGamal também é comutativo, podendo ser utilizado tanto para assinatura digital quanto para gerenciamento de chaves; assim, ele obtém sua segurança da dificuldade do cálculo de logaritmos discretos em um corpo finito.
DSA	O Digital Signature Algorithm, unicamente destinado a assinaturas digitais, foi proposto pelo NIST em agosto de 1991, para utilização no seu padrão DSS (Digital Signature Standard). Adotado como padrão final em dezembro de 1994, trata-se de uma variação dos algoritmos de assinatura ElGamal e Schnorr. Foi inventado pela NSA e patenteado pelo governo americano.

ANEXO IV

Funções	Descrição
MD5	É uma função de espalhamento unidirecional inventada por Ron Rivest, do MIT, que também trabalha para a RSA Data Security. A sigla MD significa Message Digest. Este algoritmo produz um valor hash de 128 bits, para uma mensagem de entrada de tamanho arbitrário. Foi inicialmente proposto em 1991, após alguns ataques de criptoanálise terem sidos descobertos contra a função Hashing prévia de Rivest: a MD4. O algoritmo foi projetado para ser rápido, simples e seguro. Seus detalhes são públicos, e têm sido analisados pela comunidade de criptografia. Foi descoberta uma fraqueza em parte do MD5, mas até agora ela não afetou a segurança global do algoritmo. Entretanto, o fato dele produzir uma valor hash de somente 128 bits é o que causa maior preocupação; é preferível uma função Hashing que produza um valor maior.
SHA-1	O Secure Hash Algorithm, uma função de espalhamento unidirecional inventada pela NSA, gera um valor hash de 160 bits, a partir de um tamanho arbitrário de mensagem. O funcionamento interno do SHA-1 é muito parecido com o observado no MD4, indicando que os estudiosos da NSA basearam-se no MD4 e fizeram melhorias na sua segurança. De facto, a fraqueza existente em parte do MD5, citada anteriormente, descoberta após o SHA-1 ter sido proposto, não ocorre no SHA-1. Actualmente, não há nenhum ataque de criptoanálise conhecido contra o SHA-1. Mesmo o ataque da força bruta torna-se impraticável, devido ao seu valor hash de 160 bits. Porém, não há provas de que, no futuro, alguém não possa descobrir como quebrar o SHA-1.
MD2 e MD4	O MD4 é o precursor do MD5, tendo sido inventado por Ron Rivest. Após terem sido descobertas algumas fraquezas no MD4, Rivest escreveu o MD5. O MD4 não é mais utilizado. O MD2 é uma função de espalhamento unidirecional simplificada, e produz um hash de 128 bits. A segurança do MD2 é dependente de uma permutação aleatória de bytes. Não é recomendável sua utilização, pois, em geral, é mais lento do que as outras funções hash citadas e acredita-se que seja menos seguro.

ANEXO V

Protocolo	Descrição
IPSec	Padrão de protocolos criptográficos desenvolvidos para o IPv6. Realiza também o tunelamento de IP sobre IP. É composto de três mecanismos criptográficos: Authentication Header (define a função Hashing para assinatura digital), Encapsulation Security Payload (define o algoritmo simétrico para ciframento) e ISAKMP (define o algoritmo assimétrico para Gerência e troca de chaves de criptografia). Criptografia e tunelamento são independentes. Permite Virtual Private Network fim-a-fim. Futuro padrão para todas as formas de VPN.
SSL e TLS	Oferecem suporte de segurança criptográfica para os protocolos NTTP, HTTP, SMTP e Telnet. Permitem utilizar diferentes algoritmos simétricos, message digest (hashing) e métodos de autenticação e gerência de chaves (assimétricos).
PGP	Inventado por Phil Zimmermman em 1991, é um programa criptográfico famoso e bastante difundido na Internet, destinado a criptografia de e-mail pessoal. Algoritmos suportados: hashing: MD5, SHA-1, simétricos: CAST-128, IDEA e 3DES, assimétricos: RSA, Diffie-Hellman/DSS. Versão mais recente: 6.5.3.
S/MIME	O S/MIME (Secure Multipurpose Internet Mail Extensions) consiste em um esforço de um consórcio de empresas, liderado pela RSADSI e pela Microsoft, para adicionar segurança a mensagens eletrônicas no formato MIME. Apesar do S/MIME e PGP serem ambos padrões Internet, o S/MIME deverá se estabelecer no mercado corporativo, enquanto o PGP no mundo do mail pessoal.
SET	O SET é um conjunto de padrões e protocolos, para realizar transações financeira seguras, como as realizadas com cartão de crédito na Internet. Oferece um canal de comunicação seguro entre todos os envolvidos na transação. Garante autenticidade X.509v3 e privacidade entre as partes.
X.509	Recomendação ITU-T, a especificação X.509 define o relacionamento entre as autoridades de certificação. Faz parte das séries X.500 de recomendações para uma estrutura de diretório global, baseada em nomes distintos para localização. Utilizado pelo S/MIME, IPSec, SSL/TLS e SET. Baseado em criptografia com chave pública (RSA) e assinatura digital (com hashing).

BIBLIOGRAFIA

Manuais e livros consultados

1. Using the internet (Third Edition)
   Jerry Honeycutt
   Mary Ann Pike With 1996
2. Computer viruses and anti-virus
   Warfare - Jan Hrut Ski - 1990
3. Princípios de telecomunicações
   Jair Cândido de Melo - 1981
4. Computer Are Chi Texture and Organization
   John P. Hayes - 1988
5. Fundamentos de Radioelectrónica F.G. Petrov
   Editorial Mir Moscú. 1985
6. Códigos com Base Irracional.
   Stakhov AP, Petrosiu Y.
   Mathematica Statstica, Informática. UEM - DMI 1994
7. Uso dos códigos com base Irracional nos conversores Digitais Analógicos. Stakhov
   A.P, Petrossuik Y; Sotomane C. Mathematica Statistica Informática.
   UEM - DMI 1996
8. Cryptographs an Introduction to computer security
   De Jennifer Seberry
   Josef Pieprzyk
9. Digital computer Fundamentals
   Tomas C. Bartee 1990
10. Electrónica Digital
    Ivan Capuano 1980

BIBLIOGRAFIA ON-LINE

11. http: // www.buriti.com.br/ asd/index trabalho.htm

12. http:// www.cabalt.com

13. a http: // br. geocities.com / Sasonbs - 1917 / segurança / cripto.html

14. http: // www.gta.ufrjbr/grad/99

15. http: // br.geocites.com/gasonbs - 1917 segurança / politica.html

16. http: // ww.sabernet.net/tools/index.html